

Samoa

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction are primarily the result of low-level fraud and theft. However, according to law enforcement intelligence sources, criminal organizations based in Hawaii and California are involved in the trafficking of cocaine, MDMA and crystal methamphetamine into the island nations including Samoa. Additionally, South American and Australian based organizations use the South Pacific islands as transshipment locations for cocaine being shipped from South America into Australia and New Zealand.

The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small. The Government of Samoa (GOS) initially enacted the Money Laundering Prevention Act (the Act) in 2000 that was repealed and replaced by the new Money Laundering Prevention Act 2007. This law criminalizes money laundering associated with numerous crimes sets measures for the prevention of money laundering and requires related financial supervision. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed Western Samoa Tala (WST) one million (approximately U.S. \$354,000), a term of imprisonment not to exceed seven years, or both. This penalty is not found in the 2007 Act itself but derives from the separate Proceeds of Crime Act of 2007, which includes specific penalties for money laundering.

The Act requires financial institutions to report transactions considered suspicious to the Samoa Financial Intelligence Unit (FIU) established by the Money Laundering Prevention Authority presently under the auspices of the Governor of the Central Bank. The FIU receives and analyses disclosures from either a local financial or government institution or agency (either domestic or of a foreign state). If it establishes reasonable grounds to suspect that a transaction is suspicious, it may disclose the report to an appropriate local or foreign government or law enforcement agency. A Money Laundering Prevention Task Force (MLPTF) is established under the new Act to advise or make recommendations to the MLPA. More importantly, the MLPTF is tasked to ensure close liaison and cooperation and coordination between various GOS departments and corporations. In 2003, Samoa established under the authority of the Ministry of the Prime Minister an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to establish and maintain with appropriate backup or recovery all business transactions records and correspondence records for a minimum of five years, and to identify and verify a customer's identity when establishing a business relationship; when there is a suspicion of a Money Laundering offense or terrorist financing; or when there is doubt about the veracity or adequacy of the customer identification, or verification, documentation, or information previously obtained.

Section 31 of the Act requires that all financial institutions have an obligation to appoint a compliance officer responsible for ensuring compliance with the Act, and to establish and maintain procedures and systems to implement customer identification requirements, implement record keeping, retention, and reporting requirements and to make its officers and employees aware of procedures, policies and audit systems. Each financial institution is also required to train its officers, employees and agents to recognize suspicious transactions. A financial institution required to be audited must incorporate compliance with the MLPA 2007 as part of its audit to be confirmed by the auditor. Currency reporting at the border requires any person leaving or entering Samoa with more than \$20,000 or other prescribed amount in cash or negotiable bearer instruments (in Samoan currency or equivalent foreign

currency) either on their person or in their personal luggage to report this to the Financial Intelligence Unit.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the Samoa International Finance Authority (SIFA) and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The SIFA has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial jurisdiction with six offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the six offshore banks, Samoa currently has 25,383 international business corporations (IBCs) three international insurance companies, seven trustee companies, and 182 international trusts. Section 19 of the International Banking Act requires the directors and Chief Executive to be “fit and proper” and prohibits any person from applying to be a director, manager, or officer of an offshore bank who has been sentenced for an offense involving dishonesty. The prohibition is also reflected in the application forms and personal questionnaire that are completed by prospective applicants that detail the licensing requirements for offshore banks. The application forms list the required supporting documentation for proposed directors of a bank. These include references from a lawyer, accountant, and a bank, police clearances, curriculum vitae, certified copies of passports, and personal statements of assets and liabilities (if also a beneficial owner). The Inspector of International Banks must be satisfied with all supporting documentation that a proposed director is “fit and proper” in terms of his integrity, competence and solvency, which is defined in section 3 of the Act.

International cooperation can occur in several ways under the provisions of three pieces of legislation: the Money Laundering Prevention Act 2007, the Proceeds of Crime Act 2007, and Mutual Assistance in Criminal Matters Act 2007. All cooperation under the MLPA is through the Financial Intelligence Unit (FIU) under the new Money Laundering Prevention Act 2007, which allows exchange of information not only on a national but also on an international basis between the FIU and other domestic law enforcement and regulatory agencies. Under the Proceeds of Crime Act 2007, a foreign State can request assistance to issue a restraining order in respect of a foreign serious offense. The Attorney General under the Mutual Assistance in Criminal Matters Act 2007 can authorize the giving of assistance to a foreign state. Assistance to a foreign state can be in the form of locating or identifying persons or providing evidence or producing documents or other articles in Samoa. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2007 and the Prevention and Suppression of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Islands Forum. Samoa hosted the annual plenary of the Pacific Islands Forum in August 2004. Samoa has not signed the 1988 UN Drug Convention or the UN Convention against Transnational Organized Crime. Samoa became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. However there is no information to indicate whether Samoa circulates either the UNSCR 1267 or the U.S. lists of designated terrorist entities.

The Financial Intelligence Unit (FIU) within the Central Bank has continued to strengthen its anti-money laundering regime as evident in the new Money Laundering Prevention Act 2007. The new Act is explicitly mandates that all financial institutions conduct customer due diligence and prohibit any transactions where there is no satisfactory evidence of a customers identity. A financial institution is obliged to keep records of all business transaction records and related correspondence, records of a customer's identity, and of all reports made to the FIU, and any enquiries made to it by the FIU on money laundering and terrorist financing matters. Anonymous accounts are strictly prohibited, and transactions are required to be monitored by financial institutions. The scope of record keeping by financial institutions (like banks and money transmission service providers) is extended to include accurate originator information and other related messages made via electronic fund transfers.

The Government of Samoa (GOS) has made progress in developing its anti-money laundering/counter-terrorist finance regime in 2007 by enacting the Money Laundering Prevention Act. The GOS should ensure that financial institutions submit suspicious transaction reports (STRs) to the FIU and that the FIU forwards any STR worthy of investigation to law enforcement for possible prosecution. The GOS should effectively regulate its offshore financial sector by ensuring that the names of the actual beneficial owners of international business companies and banks are on a registry accessible to law enforcement. The GOS should ensure that the UNSCR 1267 Sanctions Committee Consolidated and U.S. lists are circulated and an effective asset forfeiture regime is established and implemented. The GOS should adhere to the FATF's 9 Special Recommendations on Terrorist Financing. In particular, Samoa should take steps to implement Special Recommendation IX on cash couriers and ensure that its entry and exit points are not used for either the transshipment of narcotics, the sale of imported narcotics, or the funds derived from either illicit activity.

Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little known narcotics related money laundering in the Kingdom. Saudi officials acknowledge difficulty in detecting terrorist financing due to the abundance of cash funds in the country. All eleven commercial banks in Saudi Arabia operate as standard "western-style" financial institutions and all banks operate under the supervision of the central bank, Saudi Arabian Monetary Agency (SAMA). Saudi Arabia is not an offshore financial center. There are no free zones for manufacturing, although there are bonded transit areas for the trans-shipment of goods not entering the country. There was no significant increase in financial crimes during 2007, although the proceeds of crime from stolen cars and counterfeit goods are substantial. A definitive determination is hard to make because of the absence of official criminal statistics.

Saudi donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. However, the Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission") found no evidence that either the Saudi Government, as an institution, or senior Saudi Government officials individually, funded al-Qaida. Following the al-Qaida bombings in Riyadh on May 12, 2003, the Saudi Arabian government (SAG) has taken significant steps to counteract terrorist financing.

In 2003, Saudi Arabia approved a new Anti-Money Laundering Law that for the first time contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years and adopt precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions; authorizes government prosecutors to investigate money laundering and terrorist financing; and allows for the exchange of information and

judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements.

SAMA guidelines generally correspond to the Financial Action Task Force (FATF) 40 Recommendations and the Nine Special Recommendations on Terrorist Financing. On May 27, 2003, SAMA issued updated anti-money laundering and counter-terrorist finance guidelines for the Saudi banking system. The guidelines require that banks have mechanisms to monitor all types of “Specially Designated Nationals” as listed by SAMA; that fund transfer systems be capable of detecting specially designated nationals; banks strictly adhere to SAMA circulars on opening accounts and dealing with charity and donation collection; and the banks be able to provide the remitter’s identifying information for all outgoing transfers. The guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of 100,000 Saudi Riyals (U.S. \$26,667); and develop internal control systems and compliance systems. SAMA also issued “know your customer” guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits nonresident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of SAMA. There are no bank secrecy laws that prevent financial institutions from reporting client and ownership information to bank supervisors and law enforcement authorities. The SAG provides anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

In 2003, the SAG established an anti-money laundering unit in SAMA, and in 2005 the SAG established the Saudi Arabia Financial Investigation Unit (SAFIU), which acts as the country’s financial intelligence unit (FIU) within the Ministry of Interior. Saudi banks are required to have anti-money laundering units with specialized staff to work with SAMA, the SAFIU and law enforcement authorities. All banks are also required to file suspicious transaction reports (STR) with the SAFIU. The SAFIU collects and analyzes STRs and other available information and makes referrals to the Bureau of Investigation and Prosecution, the Mabahith (the Saudi Security Service), and the Public Security Agency for further investigation and prosecution. The SAFIU is staffed by officers from the Mabahith and SAMA. The SAFIU is not yet a member of the Egmont Group of FIUs.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Some instances of money laundering and terrorist finance in Saudi Arabia have involved hawala. To help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative to create fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawala. An important advantage for the authorities in combating potential money laundering and terrorist financing in this system is that the senders and recipients of fund transfers through this formal financial sector are clearly identified. In an effort to further regulate the more than \$16 billion in annual remittances that leave Saudi Arabia, SAMA consolidated the eight largest moneychangers into a single bank, Bank Al-Bilad, in 2005.

In June 2007 the SAG enacted stricter regulations on the cross-border movement of money, precious metals, and jewels. Money and gold in excess of U.S. \$16,000 must be declared upon entry and exit from the country using official Customs forms.

Contributions to charities in Saudi Arabia usually consist of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. In 2002, Saudi Arabia announced its intention to establish a National Commission for Relief and Charitable Work Abroad (aka the Charities Commission), a mechanism that would oversee all private charitable activities abroad. Until the Charities Commission is established, no Saudi charity can send funds abroad. As of October 2007, the proposal was still under review by Saudi officials. As required by regulations in effect for over 20 years, domestic charities in Saudi Arabia are licensed, registered audited, and supervised by the Ministry of Social Affairs. The Ministry has engaged outside accounting firms to perform annual audits of charities’

financial records and has established an electronic database to track the operations of such charities. New banking rules implemented in 2003 that apply to all charities include stipulations that they can be only opened in Saudi Riyals; must adhere to enhanced identification requirements; must utilize one main consolidated account; and must make payments only by checks payable to the first beneficiary, which then must be deposited in a Saudi bank. Regulations also forbid charities from using ATM and credit cards for charitable purposes, and making money transfers outside of Saudi Arabia. According to SAG officials, these regulations apply to international charities as well and are actively enforced.

Saudi Arabia participates in the activities of the FATF through its membership in the Gulf Cooperation Council (GCC). In July 2004, reporting on the results of a mutual evaluation conducted in September 2003, the FATF concluded that the framework of Saudi Arabia's anti-money laundering regime met FATF recommendations for combating money laundering and financing of terrorism, but noted the need to implement these new laws and regulations. Saudi Arabia also supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) in November 2004 and was one of MENAFATF's original charter signatories.

It is the policy and practice of the SAG to comply with obligations under UN Security Council resolutions (UNSCR) on terrorist financing. SAMA circulates to all financial institutions under its supervision the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

The SAG is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The SAG has signed but has not yet ratified the UN Convention against Corruption. In August 2007, Saudi Arabia ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Saudi Arabia is taking steps towards enforcing its anti-money laundering/counter-terrorist finance laws, regulations, and guidelines. However, it needs to take concrete steps to establish the Charities Commission and to enhance its oversight and control of Saudi charities with overseas operations. Charitable donations in the form of gold, precious stones and other gifts should be scrutinized. There is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. The public dissemination of statistics regarding predicate offenses and money laundering prosecutions would facilitate the evaluation and design of enhancements to the judicial aspects of its AML system. The SAG should ratify the UN Convention against Corruption.

Senegal

A regional financial center with a largely cash-based economy, Senegal is vulnerable to money laundering. Reportedly, most money laundering involves domestically generated proceeds from corruption and embezzlement. Recent arrests of opposition politicians, journalists, and a corruption scandal that resulted in the early retirement, rather than prosecution of the implicated judges, illustrate these vulnerabilities. There is also concern that criminal figures launder and invest their own and their organization's proceeds from the growing West Africa narcotics trade. There is also evidence of increasing criminal activity by foreigners, such as narcotics trafficking by Latin American groups and illegal immigrant trafficking involving Pakistanis.

Dakar's active real estate market is largely financed by cash and property ownership and transfer is nontransparent. The building boom and high property prices suggest that an increasing amount of funds with an uncertain origin circulates in Senegal. Trade-based money laundering (TBML) is centered in the region of Touba, a largely autonomous and unregulated free-trade zone under the jurisdiction of the Mouride religious authority. Touba reportedly receives between U.S. \$550 and \$800

million per year in funds repatriated by networks of Senegalese traders and vendors abroad. Other areas of concern include cash, gold and gems transiting Senegal's airport and porous borders, as well as real estate investment in the Petite Cote south of Dakar.

Seventeen commercial banks operate alongside thriving micro credit and informal sectors. The Government of Senegal (GOS) is attempting to discourage its civil servants from using cash by depositing salaries into formal bank accounts, and the Banking Association has begun a publicity campaign to encourage the populace to use the formal banking system. Western Union, Money Gram and Money Express, associated with banks, compete with Senegal's widespread informal remittance systems, including hawala networks and the use of cash couriers. Small-scale, unregulated and nonlicensed currency exchange operations are also common, especially outside urban centers. The Banque de l'Habitat du Senegal (BHS), a Senegalese bank, has affiliates licensed as money remitters in the United States. New York State authorities have brought an enforcement action against BHS New York for failing to comply with anti-money laundering (AML) regulations.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the West African Economic and Monetary Union (WAEMU or UEMOA), including Senegal, and uses the CFA franc currency. The Commission Bancaire, the BCEAO division responsible for bank inspections, is based in Abidjan. However, it does not execute a full AML examination during its standard banking compliance examinations. Senegal has no offshore banking sector.

Senegal's currency control and reporting requirements are not uniform and are reportedly laxly enforced. There is no publicity about currency declaration requirements at major points of entry. Nonresidents on entry must declare any currency they are transporting from outside the "zone franc" greater than one million CFA (approximately U.S. \$2,000). They must also declare monetary instruments denominated in cash in any amount. When departing Senegal, nonresidents must declare any currency from outside the franc zone greater than approximately U.S. \$1,000 as well as all monetary instruments from foreign entities. The law does not require residents to declare currency on entry; on exit, they must declare amounts any foreign currency and any monetary instruments greater than approximately U.S. \$4,000. All declarations must be in writing. Customs authorities are primarily concerned with the importation of dutiable goods. Because land border crossings are patrolled by other authorities with differing mandates, currency control is not a priority.

The legal basis for Senegal's anti-money laundering/counter-terrorist financing (AML/CTF) framework is Loi Uniforme Relative a Lutte Contre le Blanchiment de Capiteaux No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of l'UEMOA/WAEMU, all member states are bound to enact and implement the legislation. Among the union, Senegal is the first country to have the legal framework in place. Senegal has an "all crimes" approach to money laundering. Self launderers may be prosecuted and it is not necessary to have a conviction for the predicate offense. Intent may be inferred from objective factual circumstances. Criminal liability applies to all legal persons as well as natural persons.

The new legislation meets many international standards with respect to money laundering, and eclipses them in some areas such as with regard to the microfinance sector, but does not comply with all Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations. The legislation also lacks certain compliance provisions for nonfinancial institutions. Although Senegal has not passed a CTF law, the penal code was amended in March 2007 to incorporate the United National Security Council Resolution (UNSCR) requirements for terrorist financing. In July 2007, l'UEMOA/WAEMU released guidance on terrorist financing for the sub-region alongside Directive No. 04/2007/CM/UEMOA, obliging member states to pass domestic CTF legislation.

The law requires banks and other financial institutions to know their customers and record and report the identity of any engaged in significant transactions, including the recording of large currency

transactions. Banks monitor and record the origin of any deposit higher than 5 million CFA (approximately U.S. \$10,000) for a single individual account and 20 to 50 million CFA (approximately U.S. \$40,000 to 100,000) for any business account. Commercial banks in Senegal are improving their internal controls and enhancing their “know your customer” (KYC) requirements. The law also contains safe harbor provisions for individuals who file reports.

Cellule Nationale de Traitement des Informations Financiers (CENTIF), Senegal’s financial intelligence unit (FIU) became operational in August 2005. The FIU currently has a staff of 27, including six appointed members: the President of the FIU, who by law is chosen from the Ministry of Economy and Finance, and five others detailed from the Customs Service, the BCEAO, the Judicial Police, and the Ministry of Justice. Senegal’s FIU is working to improve its operational abilities and is raising the awareness of the threat of money laundering in Senegal. CENTIF has provided outreach and training for obliged entities to familiarize them with their requirements and to improve the quality and variety of STRs that the FIU receives. Senegal’s FIU has applied for membership in the Egmont Group.

The police, gendarmerie and Ministry of Justice’s judicial police are technically responsible for investigating money laundering and terrorist financing. However, in reality, CENTIF reportedly retains its information and tasks law enforcement entities to investigate or retrieve information for its cases. CENTIF reportedly does not share or disseminate its information or financial intelligence to law enforcement. In 2007, CENTIF received 71 suspicious transaction reports (STRs), mostly from banks, and referred 11 cases to the Prosecutor General who, in turn, passed the cases directly to the investigating judge. No cases have concluded, although authorities have made one arrest. Official statistics regarding the prosecution of financial crimes are unavailable. There is one known conviction for money laundering since 2005. The conviction led to the confiscation of a private villa.

The Uniform Law provides for the freezing, seizing, and confiscation of property by judicial order. In addition, the FIU can order the suspension of the execution of a financial transaction for 48 hours. The BCEAO can also order the freezing of funds held by banks. The Uniform Law allows explicitly for criminal forfeiture. There is no provision for civil forfeiture.

The BCEAO has released a Directive against Terrorist Financing. Member states must enact a law against terrorist financing, which is a Uniform Law to be adopted by all WAEMU/UEMOA members parallel to the AML law. Like the AML law, the terrorist financing law is a penal law. Each national assembly must enact enabling legislation to adopt the new terrorist finance law. The FATF-style regional body (FSRB) for the 15 members of the Economic Community of Western African States (ECOWAS) known as the Intergovernmental Action Group Against Money Laundering in West Africa (GIABA) has also drafted a uniform law, which it hopes that all of its member states will enact. Senegal is a member of this body, which evaluated Senegal in 2007.

The BCEAO and the FIU circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. To date, no entity has been identified. The WAEMU/UEMOA Council of Ministers issued a directive in September 2002 requiring banks to freeze the assets of any entities designated by the Sanctions Committee.

Senegal has entered into bilateral criminal mutual assistance agreements with France, Tunisia, Morocco, Mali, The Gambia, Guinea Bissau, and Cape Verde. Multilateral ECOWAS treaties address extradition and legal assistance among the member countries. Under the Uniform Law, the FIU may share information freely with other WAEMU/UEMOA FIUs. However, Senegal has the only operational FIU within this community. CENTIF has signed a Memorandum of Understanding (MOU) for information exchange with the FIUs of Belgium, Nigeria, Algeria and Lebanon, and is working on other accords. CENTIF is open to information exchange on a reciprocity basis and shares information with FIUs of the Egmont group even without signed MOUs. The Senegalese government and law enforcement agencies are generally willing to cooperate with United States law enforcement agencies.

The Government of Senegal (GOS) has also worked with INTERPOL, Spanish, and Italian authorities on international anti-crime operations.

Senegal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. In 2007, Senegal was ranked 71 out of 180 countries in Transparency International's Corruption Perceptions Index.

The Government of Senegal should continue to work with its partners in WAEMU/UEMOA and ECOWAS to establish a comprehensive anti-money laundering and counter-terrorist financing regime. Senegal should work on achieving transparency in its financial and real estate sectors, and continue to encourage the populace to use the formal banking system, steering them away from cash transactions. Senegal should increase the frequency and effectiveness of financial reviews and audits and continue to battle corruption. Senegal should lead its regional partners and establish better uniform control of cross-border flow of currency and other bearer-negotiable instruments for both residents and nonresidents. Senegalese law enforcement and customs authorities need to develop their expertise in identifying and investigating both traditional money laundering and money laundering within the informal economy. CENTIF should perform more outreach for obliged nonbank financial institutions to ensure a better understanding of STRs, when to file them and the information they should contain. CENTIF, law enforcement and Ministry of Justice authorities should work together to coordinate roles and responsibilities with regard to case investigation and assembly, and develop a deeper interagency understanding of money laundering and terrorist financing. Senegal should amend its AML legislation to address the remaining shortcomings, and criminalize terrorist financing.

Serbia

Serbia is not a regional financial center. At the crossroads of Europe and on the major trade corridor known as the "Balkan Route," Serbia confronts narcotics trafficking, smuggling of persons, drugs, weapons and pirated goods, money laundering, and other criminal activities. Serbia continues to be a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, corruption, tax evasion and organized crime, as well as other types of crimes. Proceeds from illegal activities are invested in all forms of real estate. Trade-based money laundering (TBML), in the form of over- and under-invoicing, is commonly used to launder money.

A significant volume of money flows to Cyprus, reportedly as the payment for goods and services. The records maintained by various government entities vary significantly on the volume and value of imports from Cyprus. According to Government of the Republic of Serbia (GOS) officials, much of the difference is due to payments made to accounts in Cyprus for goods, such as Russian oil, that actually originate in a third jurisdiction.

Serbia's banking sector is more than 80 percent foreign-owned. There is no provision in the banking law that allows the establishment of offshore banks, shell companies or trusts. Serbia has 14 designated free trade zones, three of which are in operation. Serbia established the free trade zones to attract investment by providing tax-free areas to companies operating within them. These companies are subject to the same supervision as other businesses in the country. Reportedly, there is no evidence of any alternative remittance systems operating in the country. Nor, reportedly, is there evidence of financial institutions engaging in currency transactions involving international narcotics trafficking proceeds.

Serbia's expanded definition of money laundering in the Penal Code broadens the scope of money laundering and aims to conform to international standards. This legislation also gives police and prosecutors more flexibility to pursue money laundering charges. The penalty for money laundering is a maximum of 10 years imprisonment. Under this law and attendant procedure, money laundering falls

into the serious crime category and permits the use of Mutual Legal Assistance (MLA) procedures to obtain information from abroad.

Under Serbia's 2005 revised anti-money laundering law (AMLL) obliged entities must report suspicious transactions in any amount to the FIU. The law expands those sectors subject to reporting and record keeping requirements, adding attorneys, auditors, tax advisors and accountants, currency exchanges, insurance companies, casinos, securities brokers, dealers in high value goods, real estate agencies, and travel agents to those already required to comply with the AMLL provisions. The AMLL also expands the number of entities required to collect certain information and file currency transaction reports (CTRs) with the financial intelligence unit (FIU) on all cash transactions exceeding 15,000 euros (approximately U.S. \$22,000), or the dinar equivalent. These entities must also retain records for five years. Financial institutions have realized significant improvement in their compliance, i.e., gathering and keeping records on customers and transactions. The AMLL requires obligated entities and individuals to monitor customers' accounts when they have a suspicion of money laundering, in addition to reporting to the FIU. Safe harbor provisions protect the entities with respect to their cooperation with law enforcement entities. The flow of information to the FIU has been steadily increasing, but not all entities are yet subject to implementing bylaws. The AMLL also eliminates a previous provision limiting prosecution to crimes committed within Serbian territory.

The Law on Foreign Exchange Operations, adopted in 2006, criminalizes the use of false or inflated invoices or documents to conceal the illicit transfer of funds out of the country. Serbia enacted this law in part to counter the perceived problem of import-export fraud and TBML. The Foreign Currency Inspectorate, part of the Ministry of Finance, is responsible for supervising import/export companies for compliance. The law also requires residents and nonresidents declare to Customs authorities all currency (foreign or dinars), or securities in amounts exceeding 5,000 euros (approximately U.S. \$7,000) transported across the border.

The National Bank of Serbia (NBS) has supervisory authority over banks, currency exchanges, insurance and leasing companies. The NBS has issued regulations requiring banks to have compliance and know-your-customer (KYC) programs in place and to identify the beneficial owners of new accounts. In June 2006, the NBS expanded its customer identification and record keeping rules by adopting new regulations mandating enhanced due diligence procedures for certain high risk customers and politically exposed persons. The NBS is developing similar regulations for insurance companies. The Law on Banks includes a provision allowing the NBS to revoke a bank's license for activities related to, among other things, money laundering and terrorist financing, but the NBS has not yet used this revocation authority. Although the legal framework is in place, the NBS currently lacks the expertise needed for effective bank supervision. It is building these capacities through training and staff development.

The Securities Commission (SC) supervises broker-dealers and investment funds and monitors its obligors' compliance with the AML Laws. The SC is developing regulations to implement this authority. The Law on Investment Funds and the Law on Securities and Other Financial Instruments Market provide the SC with the authority to "examine" the source of investment capital during licensing procedures.

Serbia introduced a value-added tax (VAT) in 2005, and the full impact of refund fraud associated with the administration of the VAT is still not clear. Serbia's Tax Administration lacks the audit and investigative capacity or resources to adequately investigate the large number of suspicious transactions that are forwarded by Serbia's FIU. In addition, current tax law sets a low threshold for auditing purposes and has increased the burden on the Tax Administration. This has created a situation where criminals can spend and invest criminal proceeds freely with little fear of challenge by the tax authorities or other law enforcement agencies.

The Administration for the Prevention of Money Laundering (APML) serves as Serbia's FIU. The revised AMLL elevates the status of the FIU to that of an administrative body under the Ministry of Finance. This provides more autonomy for the agency to carry out its mandate, as well as additional resources. APML has its own line item operating budget. The FIU has developed listings of suspicious activity red flags for banks, currency exchange offices, insurance companies, securities brokers and leasing companies. APML also has the authority to freeze transactions for 72 hours. The FIU has signed memoranda of understanding (MOU) on the exchange of information with the NBS and Customs and is negotiating one with the Tax Administration.

From January 1, 2007 through November 19, 2007, the FIU received 1,572 suspicious transaction reports (STRs). Nearly all of the STRs received by the FIU have been filed by commercial banks. In 2007, the FIU opened 46 cases and referred 119 cases to law enforcement, investigative agencies, or the prosecutor's office for further investigation. A total of six criminal charges were submitted for money laundering charges in 2007. The most common predicate crime is "abuse of office".

In Serbia, it is difficult to convict a suspect of money laundering without a conviction for the predicate crime. In addition, courts are unwilling to accept circumstantial evidence to support money laundering or tax evasion charges. This hampers law enforcement and prosecutorial authorities from effectively using the anti-money laundering laws. The Suppression of Organized Crime Service (SOCS) of the Ministry of Interior houses a new Anti-Money Laundering Section to counter these challenges and better focus financial investigations.

The GOS has established the Permanent Coordinating Group (PCG), an interagency working group originally tasked with developing an implementation plan for the recommendations from the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures' (MONEYVAL), first-round evaluation. Subgroups have since worked to draft amendments to the AMLL that will bring the country's laws into compliance with the European Union's Third Directive on money laundering. The PCG and the working groups meet intermittently as required for completing specific tasks. However, the GOS still lacks consistent interagency coordination.

Under the law, the GOS can, upon conviction for an offense, confiscate assets derived from criminal activity or suspected of involvement in terrorist financing. The FIU enforces the United Nations Security Council Resolution (UNSCR) 1267 provisions regarding suspected terrorist lists. Although the FIU routinely provides the UN list of suspected terrorist organizations to the banking community, examinations for suspect accounts have revealed no evidence of terrorist financing within the banking system. The SOCS, the Special Anti-Terrorist Unit (SAJ), and Gendarmerie, in the Ministry of Interior, are the law enforcement bodies responsible for planning and conducting the most complex antiterrorism operations. SOCS cooperates and shares information with its counterpart agencies in all of the countries bordering Serbia. Although Serbia has criminalized the financing of terrorism, the freezing, seizing and confiscation of assets of terrorists in accordance with UN Security Council resolutions still lacks a legal basis, pending enactment of draft anti-terrorism finance legislation. This draft law on terrorist financing, now pending Parliamentary approval, will apply all provisions of the AMLL to terrorist financing, require reporting to the FIU of transactions suspected to be terrorist financing and will create mechanisms for freezing, seizing and confiscation of suspected terrorist assets based on UNSCR provisions.

Serbia has no laws governing its cooperation with other governments related to narcotics, terrorism, or terrorist financing. Bases for cooperation include participation in Interpol, bilateral cooperation agreements, and agreements concerning international legal assistance. There are no laws at all governing the sharing of confiscated assets with other countries.

Serbia does not have a mutual legal assistance arrangement with the United States, but information exchange via a letter rogatory is standard. The 1902 extradition treaty between the Republic of Serbia and the United States remains in force. The GOS has bilateral agreements on mutual legal assistance

with 31 countries. As a member of MONEYVAL, Serbia will undergo a mutual evaluation in 2009. The FIU is a member of the Egmont Group and participates in information exchanges with counterpart FIUs including FinCEN. APML has also signed information sharing memoranda of understanding (MOUs) with eleven counterpart FIUs.

Serbia is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention Against Transnational Organized Crime. The GOS also is a party to all 12 UN Conventions and protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. Domestic implementation procedures, however, do not provide the framework for full application of Convention provisions.

Serbia should continue to work toward eliminating the abuses of office and the culture of corruption that enables money laundering and financial crimes. The GOS should take action to realize and implement the pending legislative initiatives necessary for Serbia to fully comply with international standards. These include the laws providing for the liability of legal persons and regulations applying all requirements of the AMLL to covered nonbank financial institutions. The GOS should enforce anti-money laundering regulations pertaining to money service businesses and obligated nonfinancial business and professions. Serbia should complete its supervisory scheme, and enact binding implementing regulations for the insurance and securities sectors. The GOS should also enact legislation to establish a robust asset seizure and forfeiture regime and legislation providing for the sharing of seized assets. Serbia also needs to enact and implement legislation needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and to require suspicions of terrorist financing to be reported to the FIU. The National Bank and other supervisory bodies need to enhance their knowledge and receive additional staff. On an operational level, law enforcement needs audit and investigative capacity to investigate the STRs that the FIU disseminates. Prosecutors and judges also need a better understanding of money laundering and terrorist financing to ensure successful prosecutions. Rather than address specific tasks as an ad hoc group, the PCG should meet on a regular basis to discuss issues and projects, and work to improve interagency coordination in such areas as information sharing, record keeping, and statistics.

Seychelles

Seychelles is not a major financial center. The existence of a developed offshore financial sector, however, makes the country vulnerable to money laundering. The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, developed an offshore financial sector to increase foreign exchange earnings and actively markets itself as an offshore financial and business center that allows the registration of nonresident companies. As of September 2007, there were 34,000 registered international business companies (IBCs) and 160 trusts that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), a body with board members from both the government and the private sector, registers, licenses and regulates offshore activities. The SIBA licenses and registers agents who carry out due diligence tests when registering new companies in the Seychelles offshore sector. The SIBA also regulates activities of the Seychelles International Trade Zone.

In addition to IBCs and trusts, Seychelles permits offshore insurance companies, mutual funds, and offshore banking. In November 2006, the GOS established the Non-Bank Financial Services Authority, which is responsible for regulating these sectors under the Mutual Funds Act, the Securities Act, and the Insurance Act. Three offshore insurance companies have been licensed: one for captive insurance and two for general insurance. Seychelles has one offshore bank to date: Barclays Bank (Offshore Unit). The International Corporate Service Providers Act 2003, designed to regulate all activities of corporate and trustee service providers, entered into force in 2004.

In its 2007-2017 Strategic Plan, the Seychelles Government proposes to facilitate the development of the financial services sector as a third pillar of the economy. It plans to achieve this through actively promoting Seychelles as an internationally recognized offshore jurisdiction, with emphasis on IBCs, mutual funds, special license companies and insurance companies.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalized the laundering of funds from all serious crimes, required covered financial institutions and individuals to report suspicious transactions to the Central Bank, which now houses the financial intelligence unit (FIU), and established safe harbor protection for individuals and institutions filing such reports. The AMLA also imposed record keeping and customer identification requirements for financial institutions, and provided for the forfeiture of the proceeds of crime. In October 2004, the International Monetary Fund (IMF) released a report on its 2002 financial sector assessment of the Seychelles. The IMF report noted deficiencies in the AMLA and its implementation, and recommended closing existing loopholes as well as updating the AMLA to reflect current international standards and best practices.

In May 2006, the Anti-Money Laundering Act 2006 came into force. This new legislation replaces the AMLA of 1996 and addresses many of the deficiencies cited by the IMF report. Under the new AMLA, money laundering controls, including the obligation to submit suspicious transaction reports (STRs), are applied to the same financial intermediaries as under the 1996 law, as well as nonbank financial institutions, such as exchange houses, stock brokerages, insurance agencies, lawyers, notaries, accountants, and estate agents. Offshore banks are also explicitly covered. The gaming sector is also obliged to report. However, although Internet gaming is also obligated, the law does not state explicitly that offshore gaming is covered in an identical manner. No offshore casinos or Internet gaming sites have been licensed to operate. There is no cross-border currency-reporting requirement. The 2006 AMLA discusses record-keeping and institutional protocol requirements, sets a maximum delay of two working days to file an STR, criminalizes tipping off, and sets safe harbor provisions. The new law also requires reporting entities to take “reasonable measures” to ascertain the purpose of any transaction in excess of Seychelles rupees 100,000 (approximately U.S. \$12,500), or of rupees 50,000 (approximately U.S. \$6,250) in the case of cash transactions, and the origin and destination of the funds involved in the transaction. However, it leaves open exceptions for “an existing and regular business relationship with a person who has already produced satisfactory evidence of identity”; for “an occasional transaction under rupees 50,000” (approximately U.S. \$6,250); and in other cases “as may be prescribed”.

Under the AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering. Money laundering is sanctioned by imprisonment for up to fifteen years and/or rupees 3,000,000 (approximately U.S. \$375,000) in penalties. While there have been 49 investigations, there have been no arrests or prosecutions for money laundering or terrorist financing since January 1, 2003. Of the 49 cases, eight were closed due to lack of evidence. In three cases, the suspects had left Seychelles, and in one case, the suspect had died. The remaining cases are still pending investigation.

The Financial Institutions Act of 2004 imposes more stringent rules on banking operations and brings the Seychelles’ regulatory framework closer to compliance with international standards. The law aims to ensure greater transparency in financial transactions by regulating the financial activities of both domestic and offshore banks. Among other provisions, the law requires that banks change their auditors every five years. Auditors must notify the Central Bank if they uncover criminal activity such as money laundering in the course of an audit.

The Financial Intelligence Unit (FIU) was established under Section 16 of the 2006 AMLA. The FIU operates within the Central Bank of Seychelles. Prior to the establishment of the FIU, the Bank Supervision Division of the Central Bank of Seychelles performed the duties of the FIU. The FIU is the focal point for receiving, analyzing, and disseminating reports of transactions related to money laundering or the financing of terrorism to the appropriate law enforcement and supervisory agencies in Seychelles. To support these core functions, the FIU is authorized to collect information that it considers pertinent and is also empowered to request additional information from reporting entities, law enforcement and supervisory agencies. The law provides for the FIU to have a proactive targeting section to research trends and developments in money laundering and terrorist financing. The FIU also performs examinations of the reporting entities and, in concert with regulators, issues guidance related to customer identification, identification of suspicious transactions, and record keeping and reporting obligations. The FIU is currently in the process of updating a set of guidelines on anti-money laundering/counter-terrorist financing (AML/CTF), which dates back to 1998, for the reporting entities in accordance with the requirements of the AMLA 2006. In December 2006, the Seychelles Government established a National Anti-Money Laundering Committee to better coordinate the efforts of the various law enforcement agencies in combating financial crimes. The Committee is chaired by the FIU, and comprises representatives of the Police, the Attorney General's Office, Customs, Immigration, the Seychelles Licensing Authority, and the Seychelles International Business Authority.

The FIU cannot freeze or confiscate property but can get a court order to effect an asset freeze. The courts have the authority to freeze or confiscate money or property. Judges in the Supreme Court have the authority to restrain a target from moving or disposing of his or her assets, and will do so if a law enforcement officer requests it, provided that the Court is "satisfied that there are reasonable grounds" for doing so. The Court also has the authority to determine the length of time for the restraint order and the disposition of assets, should it become necessary. Should the target violate the order, he or she becomes subject to financial penalties. Law enforcement may seize property subject to this order to prevent property from being disposed of or moved contrary to the order. The Court also is authorized to order the forfeiture of assets.

In 2004, the GOS enacted the Prevention of Terrorism Bill. The legislation specifically recognizes the government's authority to identify, freeze, and seize terrorist finance-related assets. The 2006 AMLA also makes the legal requirements applicable to money laundering applicable to suspected terrorist financing transactions. Assets used in the commission of a terrorist act can be seized and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or support other criminal activities. Both civil and criminal forfeiture are allowed under current legislation.

The Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to provide assistance in connection with a request to conduct searches and seizures relating to serious offenses under the law of the requesting state. The Prevention of Terrorism Act extends the authority of the GOS to include the freezing and seizing of terrorism-related assets upon the request of a foreign state. To date, no such assets have been identified, frozen, or seized.

The Government of Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Seychelles underwent a mutual evaluation review conducted by ESAAMLG in November 2006; however, the report has not been presented to the plenary body or finalized. The Seychelles is a party to the 1988 UN Drug Convention, the UN Convention Against Corruption, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. Seychelles circulates to relevant authorities the updated lists of names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224.

Seychelles should expand its anti-money laundering efforts by prohibiting bearer shares and clarifying the new legislation regarding the complete identification of beneficial owners. Seychelles should also clarify the legislation to state explicitly that all offshore activity is covered in the same manner and to the same degree as onshore. Seychelles should continue to work with its FIU to ensure it has the training and resources needed for outreach, analysis and dissemination, and comports with the membership criteria of the Egmont Group of FIUs. The GOS should also consider codifying the ability to freeze assets rather than issuing restraining orders, and develop a currency-reporting requirement for entry into its borders. Seychelles should participate more actively in ESAAMLG, and when the mutual evaluation report is finalized, address any further identified deficiencies.

Sierra Leone

Sierra Leone has a cash-based economy and is not a regional financial center. Government of Sierra Leone (GOSL) officials have reportedly stated that money laundering activities are pervasive, particularly in the diamond sector. Although there have been some attempts at tighter regulation, monitoring, and enforcement, in some areas significant diamond smuggling still exists. Loose oversight of financial institutions, weak regulations, pervasive corruption, and a widespread informal money-exchange and remittance system also work to create an atmosphere conducive to money laundering.

Former President Kabbah signed the Anti-Money Laundering Act (AMLA) in July 2005. The AMLA incorporates international standards, including setting safe harbor provisions, know your customer and identification of beneficial owner requirements, as well as mandatory five-year record-keeping for obliged entities. There is a currency reporting requirement for deposits larger than 25 million leones (approximately U.S. \$8,330) and no minimum for suspicious transaction reporting. The law requires that international financial transfers over U.S. \$10,000 use formal financial channels. The AMLA also institutes cross-border currency reporting requirements for cash or securities in excess of U.S. \$10,000. The law designates the Governor of the Bank of Sierra Leone as the national Anti-Money Laundering Authority.

Subject to the AMLA reporting requirements are financial sector institutions such as depository and credit institutions, money transmission and remittance service centers, insurance brokers, investment banks and businesses including securities and stock brokerage houses, and currency exchange houses. The AMLA also imposes reporting requirements on designated nonfinancial businesses and professions such as casinos, realtors, dealers in precious metals and stones, notaries, legal practitioners, and accountants.

A financial intelligence unit (FIU) exists but lacks the capacity to effectively monitor and regulate financial institution operations, and in particular lacks the technological capability necessary to maintain databases, track actors and patterns, and monitor online transactions. Law enforcement and customs authorities have limited resources and lack training. There have reportedly been a small number of arrests under the AMLA but no convictions due to lack of capacity by police investigators and judicial authorities.

The AMLA empowers the courts to freeze assets for seventy-two hours if a suspect has been charged with money laundering or if a charge is imminent. Upon a conviction for money laundering, all property is treated as illicit proceeds and can be forfeited unless the defendant can prove that possession of some or all of the property was obtained through legal means. The AMLA also provides for mutual assistance and international cooperation.

In July 2006, the Bank of Sierra Leone hosted a training workshop with the United Nations Office on Drugs and Crime and Intergovernmental Group for Action Against Money Laundering (GIABA) on strategy development for anti-money laundering and combating financing of terrorism. Workshop

participants recommended that the Bank of Sierra Leone draft a national anti-money laundering strategy and regulatory regime for reporting suspicious transactions to the FIU. Other recommendations focused on the FIU itself, including developing regulations for the operations of the FIU and establishing a system for the receipt, analysis, and dissemination of financial disclosures. Preparation of Sierra Leone's strategy paper has been delayed because new individuals are now involved with implementing the AMLA following the August 2007 parliamentary elections. As of late 2007, the Bank of Sierra Leone prepared the draft and recommended improving governance, setting up robust AMLA enforcement, reforming the financial sector and improving cooperation among local and regional institutions with regard to monitoring and reporting money laundering activities.

Workshop participants also recommended creating a special unit comprised of four staff from the police—two from the organized crime unit and two from the counterterrorism unit—to work specifically on anti-money laundering issues. They also recommended creating protocols to improve the exchange of information between the government offices involved, including the Attorney General's Office, Sierra Leone Police, National Revenue Authority, and Anti-Corruption Commission.

Sierra Leone is member of the Inter-Governmental Action Group against Money Laundering and Terrorist Financing in West Africa (GIABA), a FATF-style regional body (FSRB). The mutual evaluation report for Sierra Leone was conducted by the World Bank and discussed at the GIABA Plenary in June 2007. The GOSL is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Sierra Leone is number 150 of 180 countries listed in Transparency International's 2007 Corruption Perception Index.

President Ernest Bai Koroma was elected in September 2007 and came into office pledging to fight corruption. If the President succeeds in creating an environment and legal framework to combat corruption, there will be a positive impact on the enforcement of laws against money laundering. Although the Government of Sierra Leone has passed anti-money laundering legislation, it remains to be effectively harmonized with other legislation relating to anti-money laundering and combating financing of terrorism, including the Anti-Corruption Act, National Drug Control Act, and Anti-Terrorism Act. The GOSL must increase the level of awareness of money laundering issues throughout the country and allocate the necessary resources to facilitate the development of its anti-money laundering and counter-terrorist financing regime. Sierra Leone needs to develop implementing regulations for its legislation, institute a reporting regime, and strengthen its FIU through both training and technical assistance. The Sierra Leonean FIU should work toward membership in the Egmont Group. The GOSL should ensure that its counter-terrorist financing measures adhere to international standards. The GOSL should work to ensure that the UNSCR 1267 Sanctions Committee's consolidated list is distributed to financial institutions regularly. It needs to ratify the UN Convention against Transnational Organized Crime. Sierra Leone should also continue its efforts to counter the smuggling of diamonds and take steps to combat corruption at all levels of commerce and government.

Singapore

As a significant international financial and investment center and, in particular, as a major offshore financial center, Singapore is vulnerable to money launderers. Stringent bank secrecy laws and the lack of routine currency reporting requirements make Singapore a potentially attractive destination for drug traffickers, transnational criminals, terrorist organizations and their supporters seeking to launder money, as well as for flight capital. Structural gaps remain in financial regulations that may hamper efforts to control these crimes. To address some of these deficiencies, Singapore is implementing legal and regulatory changes to better align itself with the Financial Action Task Force's (FATF) revised

recommendations on anti-money laundering (AML) and counter-terrorist financing (CTF). FATF will conclude a Mutual Evaluation of Singapore's AML/CTF regime in February 2008.

Singapore amended the Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) in May 2006 to add 108 new categories to its "Schedule of Serious Offenses." The CDSA criminalizes the laundering of proceeds from narcotics transactions and other predicate offenses, including ones committed overseas that would be serious offenses if committed in Singapore. Included among the new offenses are crimes associated with terrorist financing, illicit arms trafficking, counterfeiting and piracy of products, environmental crime, computer crime, insider trading, and rigging commodities and securities markets. With an eye on Singapore's two new multibillion-dollar casinos slated to be operational in 2009, the list also addresses a number of gambling-related crimes. However, tax and fiscal offenses are still absent from the expanded list.

Singapore has a sizeable offshore financial sector. As of October 2007, there were 112 commercial banks in operation, including six local and 24 foreign-owned full banks, 42 offshore banks, and 40 wholesale banks. All offshore and wholesale banks are foreign-owned. Singapore does not permit shell banks in either the domestic or offshore sectors. The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Prime Minister's Office, serves as Singapore's central bank and financial sector regulator, particularly with respect to Singapore's AML/CTF efforts. MAS performs extensive prudential and regulatory checks on all applications for banking licenses, including whether banks are under adequate home country banking supervision. Banks must have clearly identified directors. Unlicensed banking transactions are illegal.

Singapore has increasingly become a center for offshore private banking and asset management. Total assets under management in Singapore grew 24 percent between 2005 and 2006 to Singapore \$891 billion (U.S. \$581 billion), according to MAS. Private wealth managers estimate that total private banking and asset management funds increased nearly 300 percent between 1998 and 2004.

Beginning in 2000, MAS began issuing a series of regulatory guidelines ("Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance and cooperate with Singapore enforcement agencies on money laundering cases. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation such as passports or identity cards from all individual customers to verify names, permanent contact addresses, dates of births and nationalities. Banks must also check the bona fides of company customers. The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. They also mandate specific record-keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. Similar guidelines and notices exist for finance companies, merchant banks, life insurers, brokers, securities dealers, investment advisors, futures brokers and advisors, trust companies, approved trustees, and money changers and remitters.

Singapore is in the process of revising its AML/CTF regulations for banks and other financial institutions. MAS issued new or revised AML/CTF regulations (in the form of "Notices" and "Guidelines") for banks and other financial institutions, most of which took effect March 1, 2007. Affected institutions include banks, finance companies, merchant banks, moneychangers and remitters, life insurers, capital market intermediaries, and financial advisers. New reporting requirements for originator information on cross-border wire transfers took effect July 1. The relevant regulations further align certain parts of Singapore's AML/CTF regime more closely with FATF recommendations and specifically address CTF concerns for the first time. Among the recently implemented regulations are new provisions that would proscribe banks from entering into, or continuing, correspondent banking relationships with shell banks; clarify and strengthen procedures for customer due diligence (CDD), including adoption of a risk-based approach; mandate enhanced

CDD for foreign politically exposed persons; and additional suspicious transaction reporting requirements. Effective November 1, 2007, Singapore increased the maximum penalty for financial institutions that fail to comply with AML/CTF regulations from Singapore \$100,000 (U.S. \$71,000) to Singapore \$1 million (U.S. \$714,000). The Act also empowers MAS to prosecute financial institution managers in cases where noncompliance is attributable to their consent, connivance or neglect. MAS is considering new regulations for holders of stored value facilities (SVF) to limit the risk of their use for illicit purposes.

In addition to banks that offer trust, nominee, and fiduciary accounts, Singapore has 12 trust companies. All banks and trust companies, whether domestic or offshore, are subject to the same regulation, record-keeping, and reporting requirements, including for money laundering and suspicious transactions. In August 2005, Singapore introduced regulations under the new Trust Companies Act (enacted in January 2005 to replace the Singapore Trustees Act) that mandated licensing of trust companies and MAS approval for appointments of managers and directors. MAS issued revised regulations that took effect April 1, 2007 that require approved trustees and trust companies to complete all mandated CDD procedures before they can establish relations with customers. Other financial institutions are allowed to establish relations with customers before completing all CDD-related measures.

Singapore amended its Moneylenders Act in April 2006 to require moneylenders under investigation to provide relevant information or documents. The Act imposes new penalties for giving false or misleading information and for obstructing entry and inspection of suspected premises. Singapore is considering further amendments to strengthen the Act's AML/CTF provisions.

Singapore has issued additional regulations and guidelines governing designated nonfinancial businesses and professions. The Internal Revenue Authority of Singapore issued AML/CTF guidelines for real estate agents in July 2007. The Law Society of Singapore in August 2007 amended its Legal Profession (Professional Conduct) Rules to strengthen its AML guidelines. Among its provisions, the new rules prohibit attorneys from acting on the behalf of anonymous clients to open or maintain bank accounts or to hold cash or cash instruments.

In April 2005, Singapore lifted its ban on casinos, paving the way for development of two integrated resorts scheduled to open in 2009. Combined total investment in the resorts is estimated to exceed U.S. \$5 billion. In June 2006, Singapore implemented the Casino Control Act. The Act establishes the Casino Regulatory Authority of Singapore, which will administer the system of controls and procedures for casino operators, including certain cash reporting requirements. Internet gaming sites are illegal in Singapore.

A person who wishes to engage in for-profit business in Singapore, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company is required to have at least two directors, one of whom must be resident in Singapore, and one or more company secretaries who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted.

Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions and are required to maintain adequate records. Since November 1, 2007, Singapore has begun requiring in-bound and out-bound travelers to report cash and bearer-negotiable instruments in excess of Singapore \$30,000 (U.S. \$20,675), in accordance with FATF Special Recommendation Nine. Violators are subject to a fine of up to Singapore \$50,000 (U.S. \$34,459) and/or a maximum prison sentence of three years.

The Singapore Police's Suspicious Transaction Reporting Office (STRO) has served as the country's Financial Intelligence Unit (FIU) since January 2000. Procedural regulations and bank secrecy laws limit STRO's ability to provide information relating to financial crimes. In December 2004, STRO

concluded a Memorandum of Understanding (MOU) concerning the exchange of financial intelligence with its U.S. counterpart, FinCEN. STRO has also signed MOUs with counterparts in Australia, Belgium, Brazil, Canada, Greece, Hong Kong, Italy, Japan, and Mexico. To improve its suspicious transaction reporting, STRO has developed a computerized system to allow electronic online submission of STRs, as well as the dissemination of AML/CTF material. It plans to encourage all financial institutions and relevant professions to participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act that took effect in January 2003 criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used (or having reasonable grounds to believe that the property will be used) to commit any terrorist act or for various terrorist purposes. The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of material assistance in preventing a terrorist financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets.

The International Monetary Fund/World Bank assessment of Singapore's financial sector published in April 2004 concluded that, because Singapore is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the country imposes few restrictions on intergovernmental terrorist financing-related mutual legal assistance, even in the absence of a Mutual Legal Assistance Treaty. However, the IMF urged Singapore to improve its mutual legal assistance for other offenses, noting serious limitations on assistance through the provision of bank records, search and seizure of evidence, restraints on the proceeds of crime, and the enforcement of foreign confiscation orders.

Based on regulations issued in 2002, MAS has broad powers to direct financial institutions to comply with international obligations related to terrorist financing. The regulations bar banks and financial institutions from providing resources and services of any kind that will benefit terrorists or terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to designated terrorists or any information on transactions involving terrorists' funds. The regulations apply to all branches and offices of any financial institutions incorporated in Singapore or incorporated outside of Singapore, but located in Singapore. The regulations are periodically updated to include names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Singapore's approximately 757,000 foreign guest workers are the main users of alternative remittance systems. As of October 2007, there were 380 moneychangers and 92 remittance agents. All must be licensed and are subject to the Money-Changing and Remittance Businesses Act (MCRBA), which includes requirements for record keeping and the filing of suspicious transaction reports. Firms must submit a financial statement every three months and report the largest amount transmitted on a single day. They must also provide information concerning their business and overseas partners. Unlicensed informal networks, such as hawala, are illegal. In August 2005, Singapore amended the MCRBA to apply certain AML/CTF regulations to remittance licensees and moneychangers engaged in inward remittance transactions. The Act eliminated sole proprietorships and required all remittance agents to incorporate under the Companies Act with a minimum paid-up capital of Singapore \$100,000 (approximately U.S. \$60,000). In July 2007, MAS issued regulations that require licensees to establish the identity of all customers. MAS must approve any non face-to-face transactions.

Singapore has five free trade zones (FTZs), four for seaborne cargo and one for airfreight, regulated under the Free Trade Zone Act. The FTZs may be used for storage, repackaging of import and export

cargo, assembly and other manufacturing activities approved by the Director General of Customs in conjunction with the Ministry of Finance.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding that can be transferred out of Singapore. Singapore had a total of 1,900 registered charities as at end 2006. All charities must register with the Commissioner of Charities that reports to the Minister for Community Development, Youth and Sports. Charities must submit governing documents outlining their objectives and particulars of all trustees. The Commissioner of Charities has the power to investigate charities, search and seize records, restrict the transactions into which the charity can enter, suspend staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records and retain them for at least seven years.

Changes to the Charities (Registration of Charities) Regulations that came into effect in May 2007 authorize the Commissioner to deregister charities deemed to be engaged in activities that run counter to the public interest. Singapore has also implemented tighter rules under the Charities Act that govern public fund-raising by charities, effective May 1, 2007. Charities authorized to receive tax-deductible donations are required to disclose the amount of funds raised in excess of Singapore \$1 million (approximately U.S. \$690,000), expenses incurred, and planned use of funds. Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations (1994), any charity or person that wishes to conduct or participate in any fund-raising for any foreign charitable purpose must apply for a permit. The applicant must demonstrate that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow for a lower percentage. Permit holders are subject to additional record-keeping and reporting requirements, including details on every item of expenditure, amounts transferred to persons outside Singapore, and names of recipients. The government issued 26 permits in 2006 and 18 permits as of November 2007 related to fundraising for foreign charitable purposes. There are no restrictions or direct reporting requirements on foreign donations to charities in Singapore.

To regulate law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. Parliament amended the MACMA in February 2006 to allow the government to respond to requests for assistance even in the absence of a bilateral treaty, MOU or other agreement with Singapore. The MACMA provides for international cooperation on any of the 292 predicate “serious offenses” listed under the CDSA. In November 2000, Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking (Drug Designation Agreement or DDA). This was the first agreement concluded pursuant to the MACMA. The DDA, which came into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover nonnarcotics-related money laundering, terrorist financing, or financial fraud.

In May 2003, Singapore issued a regulation pursuant to the MACMA and the Terrorism Act that enables the government to provide legal assistance to the United States and the United Kingdom in matters related to terrorist financing offenses. Singapore concluded mutual legal assistance agreements with Hong Kong in 2003, India in 2005, and Laos in 2007. Singapore is a party to the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters along with Malaysia, Vietnam, Brunei, Cambodia, Indonesia, Laos, the Philippines, Thailand, and Burma. The treaty will come into effect after ratification by the respective governments. Singapore, Malaysia, Laos, Vietnam and Brunei have ratified thus far.

In addition to the UN International Convention for the Suppression of the Financing of Terrorism, Singapore is also party to the 1988 UN Drug Convention. In August 2007, Singapore also ratified the UN Convention against Transnational Organized Crime. Singapore has signed, but has not yet ratified, the UN Convention against Corruption. In addition to FATF, Singapore is a member of the Asia/Pacific Group (APG) on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors.

Singapore should continue close monitoring of its domestic and offshore financial sectors. The government should add tax and fiscal offenses to its schedule of serious offenses. The conclusion of broad mutual legal assistance agreements is also important to further Singapore's ability to work internationally to counter money laundering and terrorist financing. Singapore should lift its rigid bank secrecy restrictions to enhance its law enforcement cooperation in areas such as information sharing and to conform to international standards and best practices. Singapore should ratify the UN Convention against Corruption.

Slovak Republic

The geographic, economic, and legal conditions related to money laundering in Slovakia are typical of Central European economies in transition. While not a regional financial center, Slovakia's location makes it an attractive transit country for smuggling and trafficking in narcotics, mineral oils, and people. Organized criminal activity and opportunities to use gray market channels also lead to a favorable money laundering environment. According to the Financial Police, auto theft is the most commonly prosecuted predicate offense to money laundering.

Since 2000, Slovakia has strengthened the financial provisions of its criminal and civil codes through a series of amendments, which have resulted in an increased number of money laundering prosecutions. Slovakia replaced its original anti-money laundering (AML) legislation, Act No. 249/1994, with Act No. 367/2000, On Protection against the Legalization of Proceeds from Criminal Activities, which entered into force in January 2001. The Act defines money laundering, stating that "legalization of incomes derived from illegal activities," is "the use or other disposal of income or other property acquired or reasonably suspected of being acquired from illegal activity with the knowledge or suspicion that it was acquired through criminal activity in Slovakia or a third country." The Act defines "Use or disposal of property" as "ownership, possession or use of real estate, movable property, securities, monies or other liquid assets," and "disposal of income" as a "transfer of ownership, possession or use of such property with the purpose of concealing or disguising ownership." One of the most significant concepts defined in the Act is "unusual transaction" which the Act defines as "a legal action or other action which suggests that execution may enable legalization or the financing of terrorism." In practice, both unusual and suspicious transactions need to be reported, and Slovak authorities use the terms interchangeably. The Act sets forth the powers of the financial police and defines basic responsibilities of obliged entities, imposing customer identification, record keeping, and suspicious transaction reporting requirements on financial institutions.

Act No. 367/2000 expanded the list of entities subject to reporting requirements from banks and depository institutions to include foreign bank subsidiaries, the Slovak Export-Import Bank, nonbank financial institutions such as casinos, post offices, brokers, stock exchanges, commodity exchanges, securities markets, asset management companies, insurance companies, real estate companies, tax advisors, auditors, credit unions, leasing firms, auctioneers, foreign exchange houses, and pawnshops. Nonprofit organizations are generally exempt from reporting requirements.

The Government of Slovakia (GOS) amended Act No. 367/2000 to address deficiencies in the original legislation and to harmonize Slovak legislation with the Second European Union (EU) Money Laundering Directive. Amendments to Act No. 367/2000 in 2002 extend reporting requirements to include dealers of antiques, art and collectibles; precious metals and stones, and other high-value

goods; legal advisors; consultants; securities dealers; foundations; financial managers and consultants; and accounting services. The failure to report an unusual transaction is a criminal offense, punishable by 2-8 years imprisonment. Tipping off is also a criminal offense. The 2005 Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) evaluation report (MER) reported a lack of reporting on the part of designated nonfinancial business and professions (DNFBPs), and that casinos and exchange houses had not reported at all. The Slovak financial intelligence unit (FIU) estimated that of approximately 100,000 obliged entities, only banks and insurance companies had reported regularly, and the securities sector infrequently. It is unclear whether the obliged entities understand their reporting obligations. Slovakia has no requirement to give special attention to business relationships or transactions with legal or actual persons from countries not applying, or insufficiently applying, FATF recommendations.

Obliged entities must identify all customers, including legal entities, if they find the customers prepared or conducted suspect transactions, or if a sum of multiple transactions exceeding 15,000 euros (approximately U.S. \$19,000) within a 12-month period is involved. Insurance brokers must identify all clients whose premiums exceed approximately 1,000 euros (approximately U.S. \$1,400) in a year or whose one-time premium exceeds approximately 2,500 euros (approximately U.S. \$3,600). Casinos have enhanced customer identification requirements.

Each competent authority has the discretion to delay a suspect transaction for up to 48 hours. The entity may, upon request, further delay a transaction for an additional 24 hours if the financial police notify the institution that the case has been submitted to law enforcement authorities. If the suspicion turns out to be unfounded, the state assumes the burden of compensation for losses stemming from the delay.

Article 233 of the Criminal Code defines "Legalization of Proceeds from Criminal Activity" as a criminal offense. A money laundering conviction does not require a conviction for the predicate offense, and a predicate offense need not occur within the Slovak Republic to be considered as such. Slovakia amended its Criminal Procedure Code and Criminal Code in 2003 and 2005. The amendments enhance law enforcement powers by granting investigators the authority to conduct sting operations, and introduce limited provisions regarding corporate criminal liability. The revised codes contain sentencing guidelines, including 2 to 20 years for laundering illicit proceeds. Corporate liability for money laundering still does not exist in Slovakia.

As a result of amendments to the Slovak Civil Code in 2001, the Government of Slovakia (GOS) ordered all banks to stop offering passbook, or anonymous, accounts. All existing owners of anonymous accounts were required to disclose their identity to the bank and close the anonymous account by December 31, 2003. Owners of accounts that were still open could withdraw money for a three-year noninterest bearing grace period. The GOS confiscated all funds from accounts remaining after January 1, 2007, and deposited them in a fund administered by the Ministry of Finance, where they will be available for collection by the account holder until January 1, 2012. As of January 1, 2007, bearer passbook accounts ceased to exist.

Slovak law reportedly lacks effectiveness with regard to the beneficial ownership of legal persons. According to the 2005 MONEYVAL MER, "Slovakian law does not require adequate transparency concerning beneficial ownership and control of legal persons." The law does not mandate identification on the Commercial Register for beneficial owners of a company purchasing or holding shares in another registered company.

Slovak authorities have been preparing to implement the Third EU Money Laundering Directive. After consultations with the Ministry of Finance, the Ministry of Interior, and the National Bank of Slovakia, the FIU drafted new legislation to comply with the Third Directive. The new Anti-Money Laundering Act, which will fully implement the Third Money Laundering Directive and upgrade many

requirements regarding money laundering and terrorist financing, will come into force in February 2008. The new AML Act, when enacted, will replace Act No. 367/2000.

The Bureau of Organized Crime (BOC) focuses on all forms of organized crime, including narcotics, money laundering, human trafficking, and prostitution. The BOC has four regional units, each responsible for a different part of Slovakia (Bratislava, Eastern Slovakia, Western Slovakia, and Central Slovakia). The FIU is a fifth unit of this agency, but works at a national level.

Established in November 1996 as a department within the Financial Police, Slovakia's FIU, "Spravodajská Jednotka Finančnej Policie" in Slovak, was downgraded in 2005 to one of eight divisions of the BOC. The FIU has four departments: the Unusual Transactions Department, the Obligated Entities Supervision Department, the International Cooperation Department, and the Property Checks Department. The FIU receives unusual transaction reports. Despite a slight decline in staff and resources, the FIU and regional financial police increased filings, inspections, and the number of cases forwarded for prosecution.

As the organization responsible for combating money laundering, the FIU receives and evaluates unusual (suspicious) transaction reports (STRs) and collects additional information pursuant to suspicions of money laundering. If justified, the unit forwards the case to one of the regional financial police units. All supervisory authorities must inform the FIU of any violation immediately upon discovery. Once enough information has been obtained to warrant suspicion that a criminal offense has occurred, the FIU may take appropriate measures, including asking the obliged entity to delay business or financial transactions for 48 hours. The FIU then submits cases of reasonable suspicion of a criminal offence to police investigators.

In 2006, the FIU received 1,571 STRs with a total value of U.S. \$568 million. The FIU submitted fourteen cases for prosecution, including two cases outstanding from 2005. The regional units of the Financial Police submitted an additional 177 cases for prosecution. A growing number of these cases involve organized crime groups transferring funds from neighboring countries (primarily Ukraine and Hungary) to Slovakia. Most criminal prosecutions involved credit fraud. Most tax prosecutions and on-site inspections violations related to abuses of Slovakia's value added tax system. Money laundering convictions (under Article 252 of the previous Criminal Code) have gradually increased. Detailed statistics on money laundering convictions are not available. However, there were no autonomous cases of money laundering convictions, since the FIU and regional financial police tend to forward for prosecution only money laundering cases that are tied to broader organized criminal activities. No information for 2007 is available.

Section 10 of Act No. 367/2000 assigns the FIU a supervisory role, embodied by the Obligated Entities Supervision Department, over the implementation of AML measures in financial institutions. In this capacity, the FIU inspects these institutions. It also has sole supervisory authority over DNFBPs. The seven officers in the supervision department carried out 92 on-site inspections in 2006, resulting in fines with a total value of U.S. \$62,000.

Slovak law mandates forfeiture of the proceeds of crime. It does not, however, allow for forfeiture from third-party beneficiaries. The Public Prosecutor Service may order the seizure of accounts during the pre-trial proceedings stage, and can order the use of information technology for enhanced investigations under Articles 79c, 88 and 88e of the Criminal Procedure Code. In 2006, a new Confiscation Law became effective, strengthening the government's ability to seize assets gained through criminal activity.

The Law on Proving the Origin of Property came into force on September 1, 2005. According to the law, an undocumented increase in property exceeding an amount 200 times the minimum monthly wage must be scrutinized and could be considered illegal. The police must investigate allegations of illegally acquired property, and report their findings to the Office of the Public Prosecutor. The Public Prosecutor's Office may then order the property confiscated. However, the new law was controversial,

and a provisional decision of the Constitutional Court froze its implementation on October 6, 2005. A year later, the Constitutional Court suspended the Act. The Constitutional Court has not yet reached a final decision on this law.

Supporting a terrorist group is an offense under the Criminal Code. Act No. 445/2002 amended the money laundering law to criminalize terrorist financing and require obliged entities to report transactions possibly linked to terrorist financing. Although authorities have acknowledged the ability to prosecute “aiding and abetting an offense of terrorism or the establishment of a terrorist group,” no case has gone before the courts.

As Slovakia itself reported in its 2004 self-assessment questionnaire on its AML efforts, its counter-terrorist financing (CTF) regime is not fully compliant with the FATF’s Special Recommendations on Terrorist Financing. MONEYVAL gave Slovakia a rating of “partial compliance” in 2004 with regard to Special Recommendation I (Implementation of UNSCR 1373), as the criminalization of terrorist financing solely based on aiding and abetting does not meet the FATF standard; and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information). The MER also stated that Slovakia’s provisions are not broad enough to clearly criminalize the collection of funds with the intent to carry out terrorist acts, support terrorist organizations regardless of whether the donation is for the commission of a terrorist act, or for the use of any individual terrorist.

All competent authorities in the Slovak Republic have full authority to freeze or confiscate terrorist assets consistent with UNSCR 1373. The GOS has agreed to immediately freeze all accounts owned by entities listed by the UNSCR 1267 Sanctions Committee Consolidated List of terrorist entities, the EU’s consolidated lists, and those provided by the United States under Executive Order 13224. The GOS posts the lists online, but does not distribute them. Obligated entities must check the website and report any matches they find. In the event an obliged entity were to identify a terrorism-related account, the financial police could suspend any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize assets. However, the reporting obligation with respect to terrorist financing remains insufficiently clear. Obligated entities and other covered institutions have not received any guidance and no reports involving terrorist financing have been filed. Guidance and communication with financial intermediaries and DNFBPs is reportedly weak. No terrorist finance-related accounts have been frozen or seized in Slovakia.

Slovakia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. Slovakia is also a party to the European Convention on Mutual Assistance in Criminal Matters and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Slovakia is a member of the MONEYVAL Committee. Its FIU is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with seven counterpart FIUs and with the Royal Canadian Mounted Police (RCMP).

The Government of Slovakia should continue to improve its AML/CTF regime. Authorities should ensure that property and proceeds are equivalent in Article 252 and that this definition is codified to avoid confusion on this issue. Slovakia should also provide guidance and outreach to, and improve supervision of, its DNFBPs to ensure that they follow their AML and CTF reporting requirements. Slovakia should implement formal AML supervision for exchange houses. Slovak authorities should encourage and enable police to pursue money laundering and financial crime even when it does not involve organized crime activities. Slovakia should provide adequate resources to ensure that the FIU, law enforcement, and prosecutorial agencies receive adequate funding and training, as well as maintain adequate staff, to effectively perform their various responsibilities. The FIU in particular needs staffing commensurate with its responsibilities. The GOS should work to enhance cooperation and coordination among these agencies and other competent authorities. Slovakia should take steps to

include in its legislative framework the international standard for definition and treatment of beneficial owners. Authorities should also consider requiring enhanced due diligence or reporting requirements for transactions involving countries not in conformance with FATF standards, and consider adopting criminal, civil or administrative sanctions for money laundering in relation to legal persons. The GOS should consider amending its confiscation and forfeiture regime to provide for asset forfeiture from third-party beneficiaries.

The Government of Slovakia should hone its legal framework to clarify the reporting obligation with respect to terrorist financing and issue formal guidance to covered institutions. The GOS should ensure proactive circulation of the UN, EU and U.S. lists of terrorist entities to obliged entities, thus tightening the CTF regime. The GOS should also codify reporting requirements for charitable and nonprofit organizations. Authorities should amend the Criminal Code to ensure that the criminalization of terrorist financing parallels international standards, including broad parameters that criminalize the collection of funds for carrying out terrorist acts, for any activities undertaken by terrorist organizations, and for use by any individual terrorist.

South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, make it a very vulnerable target for transnational and domestic crime syndicates. Nigerian, Pakistani, and Indian drug traffickers, Chinese triads, Taiwanese groups, Lebanese trading syndicates, and the Russian mafia have all been identified as operating in South Africa, along with South African criminal groups. The fact that a high number of international crime groups operate in South Africa and that there are few reported money laundering prosecutions indicate that South Africa remains vulnerable to all-source money laundering. Although the links between different types of crime have been observed throughout the region, money laundering is primarily related to the illicit narcotics trade. Other common types of crimes related to money laundering are: fraud, theft, corruption, currency speculation, illicit dealings and theft of precious metals and diamonds, human trafficking, stolen cars, and smuggling. Most criminal organizations are also involved in legitimate business operations. There is a significant black market for smuggled goods.

South Africa is not an offshore financial center, nor does it have free trade zones. It does, however, operate Industrial Development Zones (IDZs). The South African Revenue Service (SARS) monitors the customs control of these zones. Imports and exports that are involved in manufacturing or processing in the zone are duty-free, provided that the finished product is exported. South Africa maintains IDZs in Port Elizabeth, East London, Richards Bay, and Johannesburg International Airport.

The Proceeds of Crime Act (No. 76 of 1996) criminalized money laundering for all serious crimes. This act was repealed and replaced by the Prevention of Organized Crime Act (no. 121 of 1998), which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Violation of this act carries a fine of up to 100 million rand (approximately U.S. \$14.8 million) or imprisonment for up to 30 years.

The Financial Intelligence Centre Act (FICA) requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Regulated businesses include companies and firms considered particularly vulnerable to money laundering activities, such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, it forwards this information to the investigative and prosecutorial authorities. If there is suspicion of terrorist financing, that information is to be forwarded to the National Intelligence Service. There are no bank secrecy laws in effect that prevent the

disclosure of ownership information to bank supervisors and law enforcement authorities. Regulations require suspicious transaction reports to be sent to the South African financial intelligence unit (FIU), the Financial Intelligence Centre (FIC). Both the Prevention of Organized Crime Act and the FICA contain criminal and civil forfeiture provisions.

The FIC began operating in February 2003. The mandate of the FIC is to gather and analyze financial intelligence for use against money laundering and other financial crimes; to coordinate policy and efforts to counter money laundering activities; and to act as a centralized repository of information and statistics on money laundering. The FIC is a member of the Egmont Group of financial intelligence units. In addition to the FIC, South Africa has a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance on policies and measures to combat money laundering.

From March 2006 through March 2007, the FIC received 21,466 suspicious transaction reports (STRs), an increase of nine percent from the previous year's 19,793 STRs. Eighty-eight percent of the reports came from financial institutions, with the balance coming from casinos, coin dealers, accountants, attorneys, and other reporting entities. FIC referred 549 STRs to law enforcement and/or intelligence agencies for further investigation, with a value in excess of 1.4 billion rand (approximately U.S. \$200 million). FIC and banking officials report that the quality of STRs is steadily improving, as bank personnel receive AML training and as AML software and other detection systems are installed and refined.

Precise information is not available on how many of the STRs led to criminal investigations. However, the number of money laundering and terrorist finance investigations, prosecutions, and convictions is thought to be very low. Two of the corporate defendants in the high-profile 2005 Schabir Shaik corruption trial were convicted of money laundering. However, the small number of actual cases prosecuted in South Africa indicates problems in reporting, analysis, and investigations. Many investigators and prosecutors seem to focus on the underlying "predicate" crimes, and may be unfamiliar with money laundering offenses or see no reason to add money laundering charges to cases.

In 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act came into effect. The Act criminalizes terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity. The Act is applicable to charitable and nonprofit organizations operating in South Africa. The Act requires financial institutions to report suspected terrorist activity to the FIC. The FIC distributes the list of individuals and entities included on the United Nations (UN) 1267 Sanctions Committee's consolidated list.

Conforming to the new money laundering regime has been expensive for banks, which have re-registered customers, given AML training to thousands of employees, expanded their internal compliance offices, and taken other steps to meet global best practices and comply with the law. Many banks state that the reporting requirements hamper their efforts to attract new customers. For example, if the customer has never traveled outside the country, they may not have supporting documentation (no driver's license or passport) to properly satisfy the due diligence laws. Also, retroactive due diligence requirements mean those account holders who do not present identifying documents in person risk having their accounts frozen. These requirements were fully implemented in September 2006, after which date transactions with accounts owned by still-unidentified persons were blocked. Reporting requirements were specifically waived for brokers assisting clients with a one-time amnesty offer according to the Exchange Control and Amnesty and Amendment of Taxation Laws of 2003.

Because of the cash-driven nature of the South African economy, alternative remittance systems that bypass the formal financial sector exist and are used largely by the Islamic and Indian communities. Hawala networks in South Africa have direct ties to South Asia and the Middle East. Currently, there is no legal obligation requiring alternative remittance systems to report cash transactions within the country.

SARS requires all visitors with cash in their possession to declare the amount upon arrival in South Africa. In addition, all South Africans and residents leaving the country with cash must declare amounts in excess of 175,000 rand (approximately U.S. \$24,600) for individuals, or 250,000 rand (approximately U.S. \$35,280) for families. Although bulk-cashing smuggling is not illegal per se, failure to make the required declarations carries a penalty. Smuggling and border enforcement are major problems in South Africa. The Financial Action Task Force (FATF) conducted a mutual evaluation of South Africa in 2003 and made several recommendations regarding controls on cross-border currency movement, thresholds, and amendments to the Exchange Control Act. While legislation has been adopted in response to the recommendations, full implementation has yet to take place.

South Africa has cooperated with the United States in exchanging information related to money laundering and terrorist financing. The two nations have a mutual legal assistance treaty and a bilateral extradition treaty. In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force (FATF), and it held the FATF Presidency for the period June 2005-June 2006. South Africa is also an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. South Africa is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The South African Government should fully implement FATF Special Recommendation Nine and establish control over cross-border currency movement. South Africa should increase steps to bolster border enforcement and should examine forms of trade-based money laundering and informal value transfer systems. It should also regulate and investigate the country's alternative remittance systems. There is an over-reliance on STR reporting to initiate money laundering investigations. Law enforcement and customs officials should follow the money and value trails during the course of their investigations. South Africa should continue to enforce anti-money laundering regulations within the casino industry. It should fully implement the new law (Protection of Constitutional Democracy against Terrorist and Related Activities Act) against terrorist activity and terrorist financing. South Africa should publish the annual number of money laundering and terrorist financing investigations, prosecutions, and convictions.

Spain

Spain is a major European center of money laundering activities as well as a major gateway for illicit narcotics. Drug proceeds from other regions enter Spain as well, particularly proceeds from hashish entering from Morocco and heroin entering from Turkey. There are no known currency transactions of significance involving large amounts of U.S. currency and/or direct narcotics proceeds from U.S. sales.

Tax evasion in internal markets and the smuggling of goods along the coastline also continue to be sources of illicit funds in Spain. The smuggling of electronics and tobacco from Gibraltar remains an ongoing problem. Airline personnel traveling from Spain to Latin America reportedly smuggle sizeable sums of bulk cash. Additional money laundering activities found in Spain include Colombian companies purchasing goods in Asia and selling them legally at stores run by drug cartels in Europe. Credit card balances are paid in Spanish banks for charges made in Latin America, and money deposited in Spanish banks is withdrawn in Colombia through ATM networks.

An unknown percentage of drug-trafficking proceeds are invested in Spanish real estate, particularly in the booming coastal areas in the south and east of the country. Up to thirty percent of the 500 euros notes in use in Europe are reported to be in circulation in Spain, directly linked to the purchase of real estate to launder money. Given the burgeoning profitability of the construction sector over the past

several years, many coastal municipalities have ignored the illegality of various construction projects in their localities. In 2006, the prosecutor's office in the southern province of Malaga processed more than 200 reports of abuse and systemic corruption related to the real estate and construction industries, resulting in judicial action against 20 out of 100 mayors in that province.

Throughout 2007, Spanish authorities conducted numerous anti-money laundering (AML) and counter-terrorist financing (CTF) operations that resulted in arrests. On July 25, Spanish authorities arrested two Syrian nationals accused of funneling donations from Muslim extremists living in Spain to foreign Islamic terrorist organizations. The network reportedly also funneled donations into the booming Spanish real estate market, selling the properties at a later date for profit. On July 27, Spanish police in cooperation with Colombian authorities dismantled a drug trafficking and money laundering network. The operation led to nine arrests in Barcelona and 18 in Colombia, along with the seizure of funds and illicit narcotics. There was little legislative activity regarding anti-money laundering and terrorism finance in 2007, though regulations clarifying financial reporting requirements were passed.

The most recent mutual evaluation of Spain was conducted by the Financial Action Task Force (FATF) in 2005, with the mutual evaluation report (MER) released in June 2006. The MER noted areas where Spain is not in full compliance with the 40 Recommendations and Nine Special Recommendations. Of the 49 recommendations, of which 47 were applicable, Spain was rated "largely compliant" or better in 32 and compliant in the five core FATF recommendations (Recommendations 1, 5, 10, 13, and Special Recommendations II and IV).

Spanish authorities recognize the presence of alternative remittance systems. Informal nonbank outlets such as "locutorios" (communication centers that often offer wire transfer services) are used to move money in and out of Spain by making small international transfers for members of the immigrant community. Spanish regulators also note the presence of hawala networks in the Islamic community.

Spain is not considered to be an offshore financial center and does not operate any free trade zones. Spanish law states that an entity can perform banking activity if its registered office, administration, and management reside within Spanish territory. Spanish law does not prohibit financial institutions from entering into banking relationships with shell banks, but there are no shell banks in Spain. Financial institutions have no requirement to determine whether a correspondent financial institution in a foreign country allows accounts used by shell banks. The Government of Spain (GOS) has no accurate estimate of the numbers of offshore banks, offshore international business companies, exempt companies, or shell companies. Spanish law does not recognize trusts, including those created in foreign countries. Offshore casinos and Internet gaming sites are forbidden, but online casinos often run from servers located outside of Spanish territory. Spanish politicians have been critical of Gibraltar's role in this regard. In this instance, regulation can only occur through mutual judicial assistance or international agreements.

Money laundering is criminalized by Article 301 of the Penal Code, added in 1988 when laundering the proceeds from narcotics trafficking was made a criminal offense. Individuals in fiduciary institutions can be held liable if their institutions have been used to commit financial crimes; a 1991 amendment made such persons culpable for both fraudulent acts and negligence connected with money laundering. The law was expanded in 1995 to cover all serious crimes that required a prison sentence greater than three years. Amendments to the code on November 25, 2003, which took effect on October 1, 2004, made all forms of money laundering financial crimes. Any property, of any value, can form the basis for a money laundering offense, and a conviction or a prosecution for a predicate offense is not necessary to prosecute or obtain a conviction for money laundering. Spanish authorities can also prosecute money laundering based on a predicate offense in another country, if the predicate offense would be illegal in Spain.

Law 19/2003 obliges financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 30,000 euros (approximately \$43,800). The

law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros (approximately U.S. \$117,520). Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros (approximately U.S. \$8,760). Foreign exchange and money remittance entities must report on transactions above 3,000 euros (approximately U.S. \$4,380). Authorities also require reporting transactions exceeding 30,000 euros (approximately U.S. \$43,800) from or with persons in countries or territories considered to be tax havens. Law 19/2003 allows the seizure of up to 100 percent of the currency if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash couriers since the law's enactment in July 2003. When the money has not been declared and cannot be connected to criminal activity, authorities may seize it until the origin of the funds is proven. On October 26, 2005, the European Parliament and the Council passed Regulation 1889/2005 on Controls of Cash Entering or Leaving the Community, which requires all travelers entering or leaving the EU with €10,000 or more in cash to declare the sum to Customs. As of June 15, 2007, all Member States were required to implement the regulation.

The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. Spanish financial institutions are required by law to maintain fiscal information for five years and mercantile records for six years.

Money laundering controls apply to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, postal services, currency exchange outlets, and individuals and unofficial financial institutions exchanging or transmitting money. Most categories of designated nonfinancial businesses and professions (DNFBPs) are subject to the same core obligations as the financial sector. The list of DNFBPs includes realty agents, dealers in precious metals and stones, as well as in antiques and art, legal advisors, accountants, auditors, lawyers, notaries and casinos

Reporting entities are required to examine and commit to writing the results of an examination of any transaction, irrespective of amount, which by its nature may be linked to laundering of proceeds. Law 12/2003 reaffirms the obligation of reporting suspicious activities. Reporting entities are required to report each suspicious transaction to the financial intelligence unit (FIU). Financial institutions also have an obligation to undertake systematic reporting of unusual transactions and those exceeding the currency threshold, including physical movements of cash, travelers' checks, and other bearer instruments/checks drawn on credit institutions above 30,000 euros (approximately U.S. \$43,795). The reporting obligation applies to the laundering of proceeds of all illicit activity punishable by a minimum of three years imprisonment, including terrorism or terrorist financing. Nonbank financial institutions (NBFIs) such as insurers, investment services firms, collective investment schemes, pension fund managers, and others are subject to these requirements.

Article 4 of Law 19/1993 and Article 15 of Royal Decree (RD) 925/1995 contain safe harbor provisions. Financial institutions and their staff are legally protected from any breach of restrictions on disclosure of information when reporting suspicious transactions. Reporting units must also take appropriate steps to conceal the identity of employees or managers making suspicious transaction reports (STRs).

The FATF MER noted shortcomings in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. Anonymous accounts and accounts in fictitious names are precluded by Spanish legislation. Bearer shares are permitted in Spain, although they are not as prevalent as they have been in the past. Spanish authorities have taken steps to neutralize them since 1998, ensuring that mere possession cannot serve as proof of ownership. However, they still exist, and the MER cited the requirements to determine the beneficial owner as "inadequate."

Law 19/1993 and RD 925/1995 established the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC) as Spain's FIU. Its primary mission is to receive,

analyze, and disseminate suspicious and unusual transaction reports from financial institutions and DNFBPs. SEPBLAC coordinates the fight against money laundering in Spain and has primary responsibility for any investigation in money laundering cases. SEPBLAC also has supervisory and inspection functions and is directly responsible for the supervision of a large number of regulated institutions; for example, it directly supervises the AML procedures of banks and financial institutions. SEPBLAC thus has memoranda of understanding with the Bank of Spain, the National Securities Market Commission, and the Director General of Insurance and Pension Funds, to coordinate with the regulators that supervise their respective sectors. SEPBLAC is an interdepartmental body chaired by the Secretary for Economic Affairs, and all of the agencies involved in the prevention of money laundering participate. The representatives include the National Drug Plan Office, the Ministry of Economy, Federal Prosecutors (Fiscalia), Customs, Spanish National Police, Civil Guard, CNMV (equivalent to the U.S. Securities and Exchange Commission), Treasury, Bank of Spain, and the Director General of Insurance and Pension Funds.

The FATF MER described the FIU's supervisory capabilities as ineffective because of its limited resources; the MER also expressed concern regarding SEPBLAC's independence from the Bank of Spain. In SEPBLAC's annual report, the organization acknowledged the weaknesses highlighted by the FATF report and expressed a desire to work to address these issues.

SEPBLAC has access to the records and databases of other government entities and financial institutions. It also has formal mechanisms in place to share information domestically and with other FIUs. SEPBLAC has been a member of the Egmont Group since 1995. In 2006, SEPBLAC received 2,251 STRs, down from 2,502 in 2005. SEPBLAC received 539 requests for information from other FIUs in 2006 and made 231 requests to Egmont members.

Any member of the Commission may request an investigation. However, the FATF MER noted some concerns about the effectiveness of SEPBLAC's investigations, stating that at certain stages of the investigative process, obtaining account files can be time-consuming. The National Police and Anticorruption Police informed the evaluation team that they receive too many reports, and the reports they do receive are not adequate to serve as the basis for an investigation. SEPBLAC delegates responsibility to a secretariat in the Treasury to carry out penalties following investigation and a guilty verdict by a court. Sanctions can include closure, fines, account freezes, or seizures of assets. Law 19/2003 allows seizures of assets of third parties in criminal transactions and a seizure of real estate in an amount equivalent to the illegal profit.

Under Spain's currency control system, individuals and companies must declare the amount, origin, and destination of incoming and outgoing funds. Cash smuggling reports are shared between host government agencies. Provisional measures and confiscation provisions apply to persons smuggling cash or monetary instruments that are related to money laundering or terrorist financing. Gold, precious metals, and precious stones are considered to be merchandise and are subject to customs legislation. Failing to file a declaration for such goods may constitute a case of smuggling and would fall under the responsibility of the customs authorities.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If a charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

The Penal Code provides for two types of confiscation: generic (Article 127) and specific, for drug-trafficking offenses (Article 374). Article 127 of the Penal Code allows for broad confiscation authority by applying it to all crimes or summary offenses under the Code. The effects and instruments used to commit the offense, and the profits derived from the offense can all be confiscated. Article 127 also provides for the confiscation of property intended for use in the commission of any crime or offense. It also applies to property that is derived directly or indirectly from proceeds of crime, regardless of whether the property is held or owned by a criminal defendant or by a third party. Article

374 of the Penal Code calls for the confiscation of goods acquired through drug trafficking-related crimes and of any profit obtained. This allows for the confiscation of instruments and effects used for illegal drug dealing, as well as the goods or proceeds obtained from the illicit traffic. Consequently, all assets held by a person convicted of drug trafficking may be confiscated if those assets are the result of unlawful conduct.

A judge may impose provisional measures concerning seizures from any type of offense by virtue of the code of criminal procedure. Effects may be seized and stored by the judicial authorities at the beginning of an investigation. The Fund of Seized Goods of Narcotics Traffickers, established under the National Drug Plan, receives seized assets. The proceeds from the funds are divided, with equal amounts going to drug treatment programs and to a foundation that supports officers fighting narcotics trafficking. The division of assets from seizures involving more than one country depends on the relationship with the country in question. EU working groups determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of FATF, FATF-style regional bodies, and the Egmont Group, to coordinate the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

The banking community cooperates with enforcement efforts to trace funds and seize or freeze bank accounts. The law is unclear as to whether or not civil forfeitures are allowed. The GOS enforces existing drug-related seizure and forfeiture laws. Spain has adequate police powers and resources to trace, seize, and freeze assets. Spain disseminates limited statistics on money laundering and terrorist financing investigations, prosecutions and convictions as well as on property frozen, seized and confiscated.

A small percentage of the money laundered in Spain is believed to be used for terrorist financing. It is primarily money from the extortion of businesses in the Basque region that is moved through the financial system and used to finance the Basque terrorist group ETA. After ETA announced the end of its cease-fire in June of 2007, reports of extortion against businesses located in the Basque and Navarra regions increased greatly. The FATF MER gives Spain a favorable review with regard to countering terrorist financing. Spain has long been dedicated to fighting terrorist organizations, including ETA, GRAPO, and more recently, Al-Qaida. Spanish law enforcement entities have identified several methods of terrorist financing: donations to finance nonprofit organizations (including ETA and Islamic groups); establishment of publishing companies that print and distribute books or periodicals for the purposes of propaganda, which then serve as a means for depositing funds obtained through kidnapping or extortion; fraudulent tax and subvention collections; the establishment of "cultural associations" used to facilitate the opening of accounts and provide a cover for terrorist finance activity; and alternate remittance system transfers.

Spain complies with all EU regulations concerning the freezing of terrorist assets. Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574. Sanctions range from ten to thirty years' imprisonment with longer terms if the terrorist actions were directed against government officials. On March 6, 2001, Spain's Council of Ministers adopted a decision requesting the implementation of UNSCR 1373 in the Spanish legal framework. EU Council Regulation (EC) 881/2002, which obliges covered countries such as Spain to execute UNSCR 1373, is implemented through EC No. 2580/of 27 December 2001. Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. In addition to the EU Council Regulations, Law 12/2003, when implemented, will allow the freezing of any type of financial flow so as to prevent the funds from being used to commit terrorist acts. Spanish authorities' ability to freeze accounts granted in the most recent law is more aggressive than that of most of their European counterparts. Though many laws are transposed from EU directives, Law 12/2003 on the prevention and freezing of terrorist financing surpasses EU Council requirements. However, the implementing regulations have yet to be announced, meaning that

Spanish authorities have not yet established and implemented a clear, efficient procedure to ensure the freezing of funds or other assets without delay.

As with all European Union countries, the obligation to freeze assets under UNSCR 1267 has also been implemented through the Council. Spain regularly circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee consolidated list. There were six actions taken against individuals or entities in 2005 under 1267 and/or 1373, for a total value of 83.75 euros (\$106). The CVAFT is charged with issuing freezing orders.

Spain is a member of the FATF and co-chairs the FATF Terrorist Finance Working Group. Spain is also involved with FSRBs as an observer to the South American Financial Action Task Force (GAFISUD) and a cooperating and supporting nation to the Caribbean Financial Action Task Force (CFATF). Spain is a major provider of counterterrorism assistance. SEPBLAC is a member of the Egmont Group and currently chairs the Outreach Committee Working Group. Spain provides AML/CTF assistance, particularly to Spanish speaking countries in Latin America.

Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. In 2007, U.S. law enforcement agencies also reported excellent cooperation with their Spanish counterparts. Spanish media gave prominent coverage to the cooperation between the U.S. Drug Enforcement Administration (DEA) and Spanish law enforcement authorities that led to the August 10, 2007 Spanish arrest of an accused prominent drug trafficker. This was one of many cases that U.S. law enforcement is working in collaboration with various Spanish authorities to resolve. In September 2007, Spanish police arrested two Pakistani men who were indicted in the U.S. on money laundering charges following a joint counter-terrorism investigation with the FBI. The investigation found evidence that more than 1 million euros (U.S. \$1.46 million) flowed from the drug trade and other criminal actions to terrorist groups.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's mutual legal assistance treaty with the United States has been in effect since 1993 and provides for sharing of seized assets "to the extent permitted by [domestic] laws." Spain has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with 14 countries around the world, as well as with the United States. SEPBLAC has bilateral agreements for cooperation and information exchange on money laundering issues with 21 FIUs around the world.

Spain is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism.

The scale of money laundering and the sophisticated methods used by criminals represent a major threat to Spain. The GOS has passed and enacted legislation designed to help eliminate and prosecute financial crimes. Spain should also review the resources available for industry supervision, and ensure that SEPBLAC has the resources it needs to effectively discharge the supervisory duties entrusted to it. The GOS should work to close the loopholes that FATF identified, including those in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. Spain should also work to implement Law 12/2003, which will greatly enhance Spain's capabilities to combat terrorist financing. Spain should maintain and disseminate statistics on investigations, prosecutions and convictions, including the amounts and values of assets frozen or confiscated.

St. Kitts and Nevis

St. Kitts and Nevis is a federation composed of two islands in the Eastern Caribbean. The federation is at major risk for corruption and money laundering due to the high volume of narcotics trafficking activity through and around the island, and the presence of known traffickers on the islands. The

growth of its offshore sector and an inadequately regulated economic citizenship program further contribute to the federation's money laundering vulnerabilities.

The Ministry of Finance oversees St. Kitts and Nevis' Citizenship by Investment Program. An individual may qualify for citizenship with a U.S. \$350,000 minimum investment in real estate. In addition, the Government of St. Kitts and Nevis (GOSKN) created the Sugar Industry Diversification Foundation (SIDF) after the closure of the federation's sugar industry as a special approved project for the purposes of citizenship by investment. To be eligible, an applicant must make a contribution between U.S. \$200,000 to \$400,000 (based on the number of the applicant's dependents). The GOSKN requires applicants to make a source of funds declaration and provide evidence supporting the declaration. According to the GOSKN, the Ministry of Finance oversees the Citizenship Investment Program and has established a Citizenship Processing Unit to manage the screening and application process.

As a federation, there is anti-money laundering, counter-terrorist financing, and offshore legislation governing both St. Kitts and Nevis. However, each island has the authority to organize its own financial structure. With most of the offshore financial activity concentrated in Nevis, it has developed its own offshore legislation independently. As of October 2007, Nevis has one offshore bank, 90 licensed insurance companies, 33,165 international business companies (IBCs), 9,840 limited liability companies (LLCs), 3,684 international trusts, 47 multiform foundations (utilized for estate planning, charity financing, and special investment holding arrangements), and 3,684 trusts. Figures from 2007 indicate that the St. Kitts has 1,201 exempt companies, 257 exempt foundations, nine exempt partnerships, 23 exempt trusts, 51 captive insurance companies, one insurance manager, five trust service providers, 25 corporate service providers, two investment companies, and three licensed Internet gaming sites. Internet gaming entities must apply for a license as an IBC.

Bearer shares are permitted provided that bearer share certificates are retained in the safe custody of authorized persons or financial institutions authorized by the Minister of Finance as approved custodians. Legislation requires certain identifying information to be maintained about bearer certificates, including the name and address of the bearer of the certificate, as well as its beneficial owner. All authorized custodians are required by law to obtain proper documents on shareholders or beneficial owners before incorporating exempt or other offshore companies. This information is not publicly available and only available to the regulator and other authorized persons who have access to the information.

The GOSKN licenses offshore banks and businesses. The GOSKN states that extensive background checks on all proposed licensees are conducted by a third party on behalf of the GOSKN before a license is granted. By law, all offshore bank licensees are required to have a physical presence in the federation; shell banks are not permitted. The Eastern Caribbean Central Bank (ECCB) has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the entire domestic sector of St. Kitts and Nevis, and for making recommendations regarding approval of offshore bank licenses. Under Section 10(8) of the Nevis Offshore Banking Ordinance, 1996 as amended in 2002, the ECCB is required to review all applications for licenses and report its findings to the Minister of Finance prior to consideration of the application.

The St. Kitts and Nevis Gaming Board is responsible for ensuring compliance of casinos. The Financial Services Commission (FSC) is the primary regulatory body for financial services in the federation and has the authority to cooperate with foreign counterparts on supervisory issues. Separate regulators for St. Kitts and Nevis carry out the actual supervision of institutions on behalf of the FSC including anti-money laundering examinations. Nevis seeks to consolidate its regulatory regime to a single unit as of January 2009, which would regulate all financial services businesses in Nevis. This would expand supervision to credit unions, local insurance companies, and money transfer agencies.

Nevis also seeks to establish a risk-based supervision program and will conduct risk assessments on all licensees, as well as establish a risk based supervision schedule for onsite and offsite monitoring.

The Proceeds of Crime Act (POCA) No. 16 of 2000 criminalizes money laundering for serious offenses (defined to include more than drug offenses), and imposes penalties ranging from imprisonment to monetary fines. The POCA also overrides secrecy provisions that may have constituted obstacles to administrative and judicial authorities' ability to access information with respect to account holders or beneficial owners. The POCA limits and monitors the international transportation of currency and monetary instruments. Any person importing into or exporting from St. Kitts and Nevis a value exceeding \$10,000 or its equivalent in Eastern Caribbean Currency needs to declare it through Customs. In addition, the Customs Control and Management Act criminalizes bulk cash smuggling. Customs and police share cash smuggling reports.

The FSC has issued guidance notes on the prevention of money laundering, pursuant to the Anti-Money Laundering Regulations. Regulations require financial institutions to identify their customers, maintain a record of transactions for up to five years, report suspicious transactions, and establish anti-money laundering training programs. The Anti-Money Laundering (Amendment) Regulations No. 36, 2001 and relevant Guidance Notes are presently under revision to include institutions' reporting obligations related to combating terrorist financing.

The Financial Intelligence Unit Act (FIUA) No. 15 of 2000 authorized the creation of a financial intelligence unit (FIU). The FIU began operations in 2001 and receives, collects, and investigates suspicious activity reports (SARs). All financial institutions, including nonbank financial institutions, are required by law to report suspicious transactions. Anti-money laundering regulations and the FIUA provide protection to reporting entities and employees, officers, owners, or representatives who forward suspicious reports to the FIU. The FIU has direct and indirect access to the records of other government entities via memorandums of understanding with domestic agencies. There is also indirect access to the records at financial institutions. The FIUA contains provisions for sharing information both domestically and with other foreign law enforcement agencies.

In 2007, the FIU received 96 SARs, almost double the number received in 2006. The FIU attributes this increase to efforts to increase awareness and educate entities of their reporting obligations. Of the 96 SARs, 40 were referred to law enforcement for appropriate action. The GOSKN did not report any action taken on these referrals. The Royal St. Kitts and Nevis Police Force is responsible for investigating financial crimes, but does not have adequate staff or training to effectively execute its mandate.

The Anti-Terrorism Act (ATA) No. 21 of 2002 provides the FIU and Director of Public Prosecutions with the authority to identify, freeze, and/or forfeit terrorist finance-related assets. However, the law only allows for criminal forfeiture. Civil forfeiture is considered unconstitutional. Under the POCA, legitimate businesses can be seized by the FIU if proven to be connected to money laundering activities. The FIU and the Director of Public Prosecutions are responsible for tracing, seizing, and freezing assets. The FIU can freeze an individual's bank account for a period not exceeding five days in the absence of a court order. The freeze orders obtained via the court at times ascribe an expiration of six months or more. Also under the POCA, there is a forfeiture fund under the administration and control of the Financial Secretary in St. Kitts and the Permanent Secretary in the Ministry of Finance in Nevis. All monies and proceeds from the sale of property forfeited or confiscated are placed in the fund to be used for the purpose of anti-money laundering activities in both St. Kitts and Nevis. Between 2001 and 2006, the GOSKN froze approximately \$2 million in assets, of which \$1 million was forfeited. No assets were seized in 2007.

The ATA criminalizes terrorist financing. The ATA also implements various UN conventions against terrorism. The GOSKN circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 sanctions committee's lists. The GOSKN has some existing

controls that apply to alternative remittance systems, but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities. To date, no terrorist related funds have been identified.

St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF) and is expected to undergo a mutual evaluation in 2008. St. Kitts and Nevis' Anti-Money Laundering/Combating Terrorist Financing Task Force will review the federation's legal and administrative structures and seek to address weaknesses in the regime in preparation for the upcoming mutual evaluation. St. Kitts and Nevis is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The FIU is a member of the Egmont Group. The GOSKN is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. St. Kitts and Nevis is not a party to the UN Convention against Corruption, and has signed, but not ratified, the Inter-American Convention against Terrorism. A Mutual Legal Assistance Treaty (MLAT) between the GOSKN and the United States entered into force in 2000.

St. Kitts and Nevis should devote sufficient resources to effectively implement its anti-money laundering regime, giving particular attention to its offshore financial sector. St. Kitts and Nevis should determine the exact number of Internet gaming companies present on the islands and provide the necessary oversight of these entities. St. Kitts and Nevis should provide adequate resources and training to law enforcement agencies to effectively investigate money laundering cases. The GOSKN should also become a party to the UN Convention against Corruption.

St. Lucia

St. Lucia has developed an offshore financial service center that is vulnerable to money laundering. Transshipment of narcotics (cocaine and marijuana), unregulated money remittance businesses, cash smuggling, and bank fraud, such as counterfeit U.S. checks and identity theft, are among the other primary vulnerabilities for money laundering in St. Lucia.

Currently, St. Lucia has six offshore banks, 2,851 international business companies (a 49 percent increase from 2006), six private mutual funds, two public mutual funds, 24 international insurance companies, 66 trust companies, three mutual fund administrators, 25 registered agents and five registered trustees (service providers), and 30 domestic financial institutions. Shell companies are not permitted. The Government of St. Lucia (GOSL) also has one free trade zone where investors may establish businesses and conduct trade and commerce within the free trade zone or between the free trade zone and foreign countries. There are no casinos or Internet gaming sites in St. Lucia and the GOSL does not plan to consider the establishment of gaming enterprises.

Money laundering in St. Lucia is a crime under the 1993 Proceeds of Crime Act and the Money Laundering (Prevention) Act (MLPA) of 2003, which superseded the Money Laundering (Prevention) Act of 1999 and the Financial Intelligence Authority Act of 2002. The MLPA criminalizes the laundering of proceeds with respect to numerous predicate offenses, including narcotics, abduction, blackmail, counterfeiting, extortion, firearms and narcotics trafficking, forgery, corruption, fraud, prostitution, trafficking in persons, tax evasion, terrorism, gambling and robbery. The MLPA mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the MLPA imposes a duty on financial institutions (which include banks, credit unions, building societies, trust companies, and financial services providers) to take reasonable measures to establish the identity of customers, and requires accounts to be maintained in the true name of the holder. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies.

The Financial Services Supervision Unit has issued detailed guidance notes to implement the MLPA. Currently, steps are also being taken to implement legislation to regulate money remitters.

In 1999, the GOSL enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act, and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. IBCs intending to engage in banking, insurance or mutual funds business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The Committee on Financial Services, established in 2001, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, the Comptroller of Inland Revenue, and others. The GOSL has implemented administrative procedures for an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates; however, the unit is not yet fully functional. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

The MLPA authorizes the establishment of St. Lucia's financial intelligence unit (FIU), which became operational in October 2003. The FIU is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) from obligated financial institutions, and has regulatory authority to monitor compliance with anti-money laundering requirements. The FIU is also able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the MLPA. Failure to provide information to the FIU is a crime punishable by a fine or up to ten years imprisonment. The FIU has access to relevant records and databases of all St. Lucian government entities and financial institutions, and is permitted by law to share information with foreign FIUs. However, no formal agreement exists for sharing information domestically and with other FIUs. In 2007, the FIU received 39 suspicious transaction reports, two of which were referred to law enforcement agencies for further investigation. There are no recorded cases of money laundering within St. Lucia's banking sector for 2007.

Customs laws criminalize cash smuggling, and customs officials are aware of cash courier problems. Cash smuggling reports are shared with the FIU, Police, Director of Public Prosecutions and the Attorney General.

Under current legislation, instruments of crime, such as conveyances, farms, and bank accounts, can be seized by the FIU. Substitute assets can also be seized. The legislation also applies to legitimate businesses if used to launder drug money, support terrorist activity, or are otherwise used in a crime. There is no legislation for civil forfeiture or shared narcotics assets. If the individual or business is not charged, then assets must be released within seven days. No assets were frozen in 2007.

The GOSL has not criminalized the financing of terrorism. However, St. Lucia circulates lists to financial institutions of terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O 13224. The GOSL has the legislative power to freeze, seize and forfeit terrorist finance related assets. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSL has been cooperative with the USG in financial crimes investigations. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty.

The GOSL is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime or the Inter-American Convention against Terrorism. The GOSL has not signed the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. St. Lucia is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. St. Lucia's FIU is not a member of the Egmont Group.

In accordance with international standards, the Government of St. Lucia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The GOSL should criminalize the financing of terrorism. It should also enhance and implement its anti-money laundering legislation and programs, including adopting civil forfeiture legislation and ensuring that its FIU meets the Egmont Group standards. The rapid expansion of the island's offshore financial services sector should be counterbalanced by efforts that increase transparency. The GOSL also needs to improve its record of investigating, prosecuting, and sentencing money launderers and those involved in other financial crimes, as well as improving and implementing its asset seizure and forfeiture regime.

St. Vincent and the Grenadines

St. Vincent and the Grenadines (SVG) remains vulnerable to money laundering and other financial crimes as a result of the rapid expansion and limited regulation of its offshore sector. Money laundering is principally affiliated with the production and trafficking of marijuana in SVG, as well as the trafficking of other narcotics from South America. Money laundering occurs in various financial institutions such as banks (domestic and offshore) and money remitters. There has been a slight increase in fraud and the use of counterfeit instruments over the last year, such as tendering counterfeit checks or cash.

The domestic financial sector includes two commercial banks, a development bank, two savings and loan banks, a building society, 16 insurance companies, 10 credit unions, and two money remitters. The offshore sector includes six offshore banks, 8,573 international business corporations (an increase of 918 from the previous year), 13 offshore insurance companies, 55 mutual funds, 27 registered agents, and 154 international trusts. There are no offshore casinos and no Internet gaming licenses have been issued. There are no free trade zones in SVG. The Government of St. Vincent and the Grenadines (GOSVG) eliminated its economic citizenship program in 2001.

No physical presence is required for offshore sector entities and businesses, with the exception of offshore banks. Nominee directors are not mandatory except when an international business corporation (IBC) is formed to carry on banking business. Bearer shares are permitted for IBCs but not for banks. The International Business Companies (Amendment) Act No.26 and 44 of 2002 was enacted to immobilize bearer shares and requires registration and custody of bearer share certificates by a registered agent who must also keep a record of each bearer certificate issued or deposited in its custody. The record must contain pertinent information relating to the company issuing the shares, the number of the share certificate, and identity of the beneficial owner. The Offshore Finance Inspector has the ability to access the name or title of a customer account and confidential information about the customer that is in the possession of a license.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's domestic banks. The International Banks (Amendment) Act No. 30 of 2002 provided the ECCB with enhanced authority to review and

make recommendations regarding approval of offshore bank license applications, and to directly supervise the offshore banks in conjunction with the International Financial Services Authority (IFSA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. The IFSA continues independently to supervise and regulate other offshore sector entities; however, its staff exercises only rudimentary controls over these institutions. The GOSVG has strengthened the structure and staffing of the IFSA to regulate offshore insurance and mutual funds. The Exchange of Information Act No. 29 of 2002 authorizes and facilitates the exchange of information among regulatory bodies.

The Proceeds of Crime and Money Laundering (Prevention) Act (PCMLPA) 2001 criminalizes money laundering, and requires financial institutions and other regulated businesses to report suspicious transactions. Reporting is required for all suspicious activities regardless of the transaction amount. In 2005, the PCMLPA was amended to expand the definition to include an all offences approach and extended the scope of sections relating to the seizure, detention, and forfeiture of cash. The Proceeds of Crime (Money Laundering) Regulations establish mandatory record-keeping rules and customer identification requirements. Financial institutions are required to maintain all records relating to transactions for a minimum of seven years.

Customers are required to complete a source of funds declaration for any cash transaction over 10,000 East Caribbean dollars (XCD) (approximately U.S. \$3,800). It is not mandatory to report other noncash transactions exceeding 10,000 XCD. In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over 10,000 XCD.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the GOSVG's financial intelligence unit (FIU). Operational as of 2002, the FIU has the mandate to receive, analyze, and investigate financial intelligence, and prosecute money laundering cases. Suspicious activity related to drug trafficking is forwarded to the Narcotics Unit for further investigation, and activity related to fraud is forwarded to the Criminal Investigation Division. The FIU also has the ability to obtain production orders and stop/freeze orders. The FIU staff includes the Director, financial investigators, legal officers, and administrative officers. As of November 2007, the FIU received 159 suspicious activity reports for the year, and more than 750 since its inception. There was one conviction for money laundering in 2007.

The FIU is the main entity responsible for supervising and examining financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. The function is also performed by the International Financial Services Authority (IFSA) and the ECCB. Money laundering controls also apply to nonbanking financial institutions and intermediaries, which the FIU monitors for compliance. Reporting entities are protected by law if fully cooperative with the FIU. An amendment to the FIU Act permits the sharing of information even at the investigative or intelligence stage. The FIU does not have direct access to the records or databases of other government entities. Generally, records are still kept in physical form and must be retrieved manually.

Existing anti-money laundering legislation allows for the criminal forfeiture of intangible as well as tangible property. Drug trafficking offenses may also be liable to forfeiture pursuant to the Drug (Prevention and Misuse) Act and the Criminal Code. There is no period of time during which the assets must be released. Frozen assets are confiscated by the FIU upon conviction of the defendant. Proceeds from asset seizures and forfeitures are placed by the FIU into the Confiscated Assets Fund established by the PCMLPA. Legitimate businesses can also be seized if used to launder drug money, support terrorist activity, or are otherwise used in a crime. A civil forfeiture bill has been drafted and is currently before the National Anti-Money Laundering Committee (NAMLC) for its approval. In 2007, approximately \$304,380 was frozen or seized. Of this amount, approximately U.S. \$69,889 was forfeited.

In 2006, the GOSVG enacted the United Nations (Anti-Terrorism Measures) (Amendment) (UNATMA) Act 2006, Act. No.13. The UNATMA criminalizes terrorist financing and imposes a legal obligation on financial institutions and relevant business to report suspicious transactions relating to terrorism and terrorist financing to the FIU. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in SVG. To date, no accounts associated with terrorists have been found. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities.

An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and the GOSVG entered into force in 1999. The FIU executes the Mutual Legal Assistance Treaty requests. A member of the Caribbean Financial Action Task Force (CFATF), the GOSVG is scheduled to undergo its second mutual evaluation in early 2008. The GOSVG is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, and the FIU is a member of the Egmont Group. The GOSVG is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOSVG has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOSVG has not signed the UN Convention against Corruption.

The Government of St. Vincent and the Grenadines has strengthened its anti-money laundering and counter-terrorist financing regime through legislation and the establishment of an effective FIU. The GOSVG should continue to ensure that this legislation is fully implemented, and that the FIU has access to all necessary information. The GOSVG should insist that the beneficial owners of IBCs are known and listed in a registry available to law enforcement, immobilize all bearer shares, and properly supervise and regulate all aspects of its offshore sector. The GOSVG should continue to provide training and devote resources to increase the cooperation among its regulatory, law enforcement, and FIU personnel in anti-money laundering and counter-terrorist financing operations and investigations. In addition, the GOSVG should consider computerizing its record keeping systems to ensure timely and effective information sharing. The GOSVG should pass civil forfeiture legislation and consider the utility of special investigative techniques. The GOSVG should also become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Suriname

Suriname is not a regional financial center. Narcotics-related money laundering is closely linked to transnational criminal activity related to the transshipment of Colombian cocaine. Domestic drug trafficking organizations and organized crime are thought to control much of the money laundering proceeds, which are “invested” in casinos, real estate, and private sector businesses. Additionally, money laundering occurs as a result of poorly regulated private sector activities, such as casinos and car dealerships, the nonbanking financial system (including money exchange businesses or “cambios”), and a variety of other means, including construction, the sale of gold purchased with illicit money, and the manipulation of commercial bank accounts.

Suriname is not an offshore financial center and has no free trade zones. There is a gold economy in the interior mining regions of the country. Suriname has a significant informal economy, the majority of which is not linked to money laundering proceeds.

A package of legislation passed in 2002 included the criminalization of money laundering. The legislation, “Reporting of Unusual Transactions in the Provision of Services,” addresses multiple issues related to all types of money laundering, including criminalizing money laundering, reporting of unusual transactions, and requiring service providers to request identification from each customer making a transaction. The legislation applies to both banking and nonbanking financial institutions. The law also provides for the establishment of a financial intelligence unit (FIU) and requires financial

institutions, nonbank financial institutions, and natural legal persons who provide financial services to report unusual transactions to the FIU. In total, approximately 130 entities in Suriname are required to report to the FIU. While the FIU has informed all entities of their reporting requirements, to date only the banking sector is in full compliance.

In accordance with international standards, objective and subjective indicators have been approved to identify unusual transactions. An unusual transaction is defined as any transaction that deviates from the usual account as well as any customer activities that are not “normal” daily banking business. Reporting is mandatory if financial transactions are above a certain threshold; however, sanctions for noncompliance are currently not enforced. The thresholds for financial institutions range from U.S. \$5,000 for money-transfer offices to U.S. \$10,000 for banks, insurance companies, money exchange offices, and savings and credit unions. Thresholds for nonbanking financial institutions and “natural legal persons” are U.S. \$5,000 for casinos, U.S. \$10,000 for dealers of precious metals and stones, and U.S. \$25,000 for notaries, accountants, lawyers, and car dealerships. In addition, service providers are required to confirm the identities of individual or corporate clients before completing requested services and to retain photocopies of identity documents and all other relevant documents pertaining to national and international transactions for a period of seven years. The legislation includes a due diligence section that holds individual bankers responsible if their institution launders money and ensures confidentiality to bankers and others with respect to their cooperation with law enforcement officials.

Statutory requirements limit the international transportation of currency and monetary instruments; amounts in excess of \$10,000 must be reported to authorities before entering or leaving Suriname. In addition, any person who wishes to take money in excess of U.S. \$10,000 out of the country must notify the Military Police. The Central Bank of Suriname also requires that all transactions in excess of U.S. \$10,000 be reported. Suriname does not recognize indigenous alternative remittance systems.

The FIU, which falls under the auspices of the Attorney General’s Office, is an administrative body that performs analytical duties. Its responsibilities entail requesting, analyzing, and reporting to the Attorney General’s office information on transactions that may constitute money laundering. If necessary, the FIU may request access to the records of other government entities. To facilitate interagency coordination, Suriname has an Anti-Money Laundering Project Team, which consists of representatives from the FIU, Judicial Police, the Attorney General’s Office, and the judiciary. Bureaucracy and the lack of financial and human resources have made it difficult for the FIU to perform to its best capabilities. On the basis of a Memorandum of Understanding (MOU), Suriname shares information regarding money laundering with the FIU in the Netherlands. Another MOU was concluded with the Netherlands Antilles in October 2007. The number of unusual transaction reports received by the FIU was not available for 2007.

Suriname’s anti-money laundering regime also includes a Financial Investigation Team (FOT) under the authority of the Judicial Police. The FOT is the body responsible for investigating all suspicious transactions identified by the FIU. Upon making a determination that an unusual activity report is indeed suspicious and sufficient to initiate an investigation, the FIU refers the matter to the Attorney General’s Office. If the Attorney General’s office concurs with the determination, it directs the FOT to conduct an investigation. Prosecutors use evidence collected from FOT investigations to build legal cases. However, the FOT suffers from a lack of personnel and resources that have rendered it largely ineffective over the past year. The 2004 sentencing of an individual to seven years imprisonment for intentional money laundering and for attempting to export a small amount of cocaine remains the most significant and longest money laundering sentence to date. Resource constraints and a severe shortage of judges are proving to be a limiting factor in expanding this success. A new class of seven judges could partially redress the problem, but they will not complete their judicial training until 2008.

While the number of prosecutions in 2007 related to money laundering was not public information, there were several significant convictions in 2007 related to illegal transfers of money. In August 2007, De Surinaamse Bank President Siegmund Proeve and former Bank President Edward Muller were sentenced to six months imprisonment for the illegal transfer of approximately U.S. \$14.5 million in casino profits to foreign countries between 1998 and 2003. The defendants were charged with transferring funds without the permission of the Foreign Exchange Commission and for the transfer of amounts over U.S. \$10,000 without reporting it to the Central Bank. Other defendants in the case were Procurement Officer Patrick Bagwandin, who was sentenced to a conditional three-month imprisonment, and Canadian Dorsett Group staffer Jeffrey Claque, who was sentenced to six months. The bank was fined U.S. \$358,000. The defendants are appealing the case and are serving their sentences while the case is under appeal.

In July 2007, a judge handed down the verdict for a 2006 case in which three people were arrested with a large sum of money and charged with money laundering. Two of the defendants were arrested after police put up a roadblock between Paramaribo and the country's most western district, Nickerie. The police seized the money and the vehicle the two were driving. The three were sentenced to 12 weeks imprisonment and each paid an additional fine of U.S. \$3,600. The prosecution filed an appeal in this case, as is possible under Suriname law, to seek a stricter sentence.

Close cooperation between Suriname and the Netherlands led to the 2005 arrest of three persons in a high profile money laundering scandal. In January 2006, one of the three was sentenced by a Dutch court to two-and-a-half years imprisonment for money laundering. In August 2006, the second suspect was convicted in Suriname, also on money laundering charges, and sentenced to one and a half years in prison. The third suspect was former Minister of Trade and Industry Siegfried Gilds, who resigned his position after the Attorney General announced he was under investigation for laundering money and membership in a criminal organization. The former Minister is alleged to have laundered close to \$1.27 million between 2003 and 2005. His trial is ongoing.

An amendment to the criminal code enacted in 2003 allows authorities to confiscate illegally obtained proceeds and assets obtained partly or completely through criminal offenses; however, assets cannot be converted to cash or disposed of until the case is settled. New assets forfeiture legislation, which would make this possible, is under consideration in Parliament. There are no provisions for civil forfeiture, and there is no legal mechanism that designates the proceeds gained by the sale of forfeited goods to be used directly for law enforcement efforts. There is no entity for the management and disposition of assets seized and forfeited for narcotics-related money laundering offenses.

The financing of terrorism is not a crime in Suriname. Suriname does have legislation that allows the authorities to freeze assets of those suspected of money laundering. The Central Bank of Suriname circulates to commercial banks the names of individuals/entities that are designated by the United Nations 1267 Sanctions Committee list as associates of Al-Qaeda, the Taliban, or Usama bin Laden. There are no known cases of charitable or nonprofit entities serving as conduits for financing terrorism in Suriname.

Upon its independence in 1975, Suriname automatically adopted an extradition treaty held between the United States and the Kingdom of the Netherlands into its own legislation, which serves as the extradition treaty between the United States and the Republic of Suriname. The GOS has an agreement with the Netherlands on extradition of nonnationals and mutual legal assistance with regard to criminal matters; but, under Surinamese law, citizens of Suriname "will not be extradited." Money laundering is an extraditable offense. Suriname has bilateral treaties and cooperation agreements with the United States on narcotics trafficking, and with Colombia, France and the Netherlands Antilles on transnational organized crime. In January 2006, Suriname, the Netherlands Antilles, and Aruba signed a Mutual Legal Assistance Agreement allowing for direct law enforcement and judicial cooperation between the countries, making it no longer necessary for the process to be first routed through The

Hague. Parties to the Agreement, which covers cooperation with regard to drug trafficking, trafficking in persons, and organized crime, had a follow-up meeting in March 2007 and expanded the cooperation to include information sharing on transnational crime and financial crimes.

Suriname is party to the 1988 UN Drug Convention and, in May 2007, acceded to the UN Convention against Transnational Organized Crime. The GOS is not a party to the UN Convention against Corruption or the Inter-American Convention against Terrorism. Draft legislation to become a party to the UN International Convention for the Suppression of the Financing of Terrorism has been prepared by the Ministry of Justice and Police, and is awaiting the Council of Ministers' approval. Suriname is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Suriname's FIU is not a member of the Egmont Group. In 2006, a joint team from the FIUs of Canada and the United States visited Suriname and agreed to sponsor Suriname's FIU in the Egmont membership process. The two organizations proposed steps to be taken by Suriname to qualify for the Egmont application process. A crucial step recommended is the formal criminalization of terrorist financing, which is a requirement for all new members of the Egmont Group.

The GOS should pass legislation to criminalize terrorist financing. Recent convictions have demonstrated the ability and willingness of the Government of Suriname to combat money laundering. However, the GOS should take steps to further enhance its anti-money laundering regime to conform to international standards. Suriname should devote the necessary resources to effectively investigate and prosecute money laundering cases. The GOS should consider implementing provisions for civil forfeiture, and create a program for the management and disposition of seized and forfeited assets. The GOS should bolster the capacity of the FIU with the necessary personnel and financial resources, and implement reforms to permit the FIU to qualify as a member of the Egmont Group.

Switzerland

Switzerland is a major international financial center. There are 331 banks and a large number of nonbank financial intermediaries. Swiss authorities suspect that Switzerland is vulnerable at the layering and integration stages of the money laundering process. Switzerland's central geographic location, relative political, social, and monetary stability, wide range and sophistication of financial services and long tradition of bank secrecy—first codified in 1934—are all factors that make Switzerland a major international financial center. These same factors also make Switzerland vulnerable to potential money launderers. However, Swiss authorities are aware of these factors and are sensitive to the size of the Swiss banking industry (14.5 percent of GDP) relative to the size of the economy. Moreover, client confidentiality laws, also called bank secrecy, are waived automatically in cases of suspected money laundering and fraud.

Reporting indicates that criminals attempt to launder criminal proceeds in Switzerland via a wide range of illegal activities conducted worldwide. These illegal activities include, but are not limited to, financial crimes, narcotics trafficking, arms trafficking, organized crime, terrorist financing and corruption. Although both Swiss and foreign individuals or entities launder money in Switzerland, foreign narcotics trafficking organizations, often based in the Balkans, Eastern Europe, or South America, dominate the narcotics-related money laundering operations in Switzerland.

Swiss bank accounts also figure in fraud and corruption of foreign government officials and heads-of-state. Recent examples of public figures that have been the subject of Swiss money laundering allegations or investigations include a former Kyrgyzstan President, a former Russian Minister of Atomic Energy, the Nigerian dictator Sani Abacha, former Pakistani Prime Minister Benazir Bhutto, and former Haiti President Jean-Claude Duvalier. These individuals have Swiss bank accounts and have moved national funds to Switzerland for personal use. Swiss bank routinely screen PEPs (Politically Exposed Persons) accounts for illicit money transfers.

Switzerland has significant anti-money laundering (AML) legislation in place, making banks and other financial intermediaries subject to strict know-your-customer (KYC) and reporting requirements. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act. Money laundering is a criminal offense in Switzerland. However, Swiss law, does not recognize certain types of criminal offenses as predicate offenses for money laundering, including illegal trafficking in migrants, counterfeiting and pirating of products, smuggling, insider trading, and market manipulation.

Swiss money laundering laws and regulations apply to both banks and nonbank financial institutions. The Federal Banking Commission, the Federal Office of Private Insurance, and the Swiss Federal Gaming Board serve as primary oversight authorities for a number of financial intermediaries, including banks, securities dealers, insurance institutions, and casinos. Other financial intermediaries are required to either come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department or join an accredited self-regulatory organization (SRO). SROs are nongovernmental self-regulating organizations authorized by the Swiss government to oversee implementation of AML measures by their members. The SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 6,000 financial intermediaries are associated with SROs; the majority of these are financial management companies.

The Swiss Federal Banking Commission's AML regulations were revised in 2002 and became effective in 2003. These regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification and install a global know-your-customer risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigations by the financial intermediary are required. The regulations require increased due diligence in the cases of politically exposed persons (PEPs) by ensuring that decisions to commence relationships with such persons be undertaken by at least one member of the senior executive body of a financial institution. All provisions apply to correspondent banking relationships as well. Swiss banks may not maintain business relationships with shell banks (banks with no physical presence at their place of incorporation), but there is no requirement that banks ensure that foreign clients do not authorize shell banks to access their accounts in Swiss banks.

The 2002 Banking Commission regulations mandate that all cross-border wire transfers must contain identifying details about the funds' remitters, though banks and other covered entities may omit such information for "legitimate reasons." The Swiss Federal Banking Commission has said that there are no plans at the moment to follow EU regulations aimed at registering names, addresses, and account numbers of everyone making even small money transfers between EU member states.

Revisions to the Swiss Penal Code regarding terrorist financing entered into force on October 1, 2003. Article 260 of the Penal Code provides for a maximum sentence of five years' imprisonment for terrorist financing. Article 100 of the Penal Code, also added in 2003, extends criminal liability for terrorist financing to include companies. The Financial Action Task Force's 2005 mutual evaluation of Switzerland found it "largely compliant" with FATF Special Recommendation II regarding the criminalization of terrorist financing; however, it noted that the Swiss Penal Code criminalizes the financing of an act of criminal violence, not the financing of an individual, independent of a particular act. The evaluation also noted that Switzerland wasn't compliant with respect to correspondent banking, beneficial ownership of legal persons, and cash couriers. On 29 September 2006 the Federal Council decided on the next steps regarding the implementation of the revised FATF recommendations to combat money laundering and terrorist financing, and on extending the scope of

the Money Laundering Act to cover terrorist financing. The adoption of anti-money laundering (AML) regulations planned for 2008-2009 will make these crimes predicate offenses.

In June 2007, the Swiss Parliament approved a new financial market regulation bill aimed at creating a new regulator to boost the image of Switzerland's financial workplace by combining the activities of three existing watchdog groups. But the Federal Financial Market Supervisory Authority (FINMA) will be delayed for a year and has been criticized in some quarters for lacking full autonomy from the government. FINMA will finally group together the regulatory work of the Federal Banking Commission, the Federal Office of Private Insurance and the Money Laundering Control Authority at the beginning of 2009. It will investigate suspected cases of money laundering and corruption. The FINMA is scheduled to become operational in early 2009.

The Swiss do not have laws comparable to those in the U.S. to report large cash transactions, cross-border currency declarations, and large cash purchases. As a result, the Swiss are unable to effectively initiate bulk cash investigations because they have no legal reporting requirement for cash into or out of Switzerland. Switzerland does have suspicious transaction reports (STRs), which are referred to law enforcement through the Money Laundering Reporting Office (MROS)—the Swiss financial intelligence unit (FIU).

Switzerland's banking industry offers the same account services for both residents and nonresidents. These can be opened through various intermediaries who advertise their services. As part of Switzerland's international financial services, banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes. Pursuant to an agreement signed between the EU and Switzerland in 2004, EU residents have tax withheld on interest payments from savings accounts based in Switzerland. This measure, enacted in concert with the EU's Savings Directive (2003/48/EC), was implemented on July 1, 2005.

Swiss commercial law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss commercial law. The financial intermediary is required to verify the identity of the beneficial owner of the stock company and must also be informed of any change regarding the beneficial owner. Bearer shares may be issued by stock companies but not by limited liability companies.

Switzerland has duty free zones. Customs authorities supervise the admission into and the removal of goods from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones; for example, export laws on strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, all apply.

Switzerland ranks fifth in the highly profitable artwork trading market, exporting SFr. 1,592 million (approximately U.S. \$1,460,000) worth of artwork in 2004. Because of the size of the Swiss art market organized crime has attempted to transfer stolen art or to use art to launder criminal funds via Switzerland. The United States is by far Switzerland's most important trading partner in this area, having purchased U.S. \$578 million worth (or 36 percent) of works of art in 2006. The 2003 Cultural Property Transfer Act, implemented in June 2005, codifies in Swiss law elements of the 1970 United Nations Educational, Scientific, and Cultural Organization (UNESCO) Convention. This measure increases from five to thirty years the time period during which stolen pieces of art may be confiscated from those who purchased them in good faith. The law also allows police forces to search bonded warehouses and art galleries.

The MROS or FIU is charged with receiving and processing suspicious transaction reports (STRs). MROS does not have any investigative powers of its own nor can it obtain additional information from reporting entities after receiving a STR. Last year, banks submitted the highest number of reports in relative terms (over 58 percent.) The payment services sector followed with 26.5 percent of all STRs filed. By canton, Zurich is on the top of the list of filing STRs with 18 percent, followed by Tessin with 14 percent and Geneva with 10 percent.

In 2006, eight reports were received by the MROS regarding terrorist finance; 20 reports were received in 2005. Out of the total number (154) of STRs submitted since 2001 in connection with suspected terrorist financing, 149 or 97 percent have been forwarded to law enforcement agencies. Suspicious activity reports were often prompted by press reports. If one compares the figures for the categories with those for 2005, it is apparent that outside information was an increasingly important factor in 2006. More than 56 percent of STRs were prompted by outside information in 2006 as opposed to 41 percent in 2005. Of these 149, 44 cases have been dropped, 5 cases have been temporarily suspended and 100 cases are still pending.

Under the 2002 Efficiency Bill, the Swiss Attorney General is vested with the power to prosecute crimes addressed by Article 340 of the Swiss Penal Code, which also covers money laundering offenses. In the past, the individual cantons (administrative components of the Swiss Confederation) were charged with investigating money laundering offences. Additional legislation increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the Federal Police and Attorney General's office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, and white collar crime.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. Under Swiss law, suspect assets may be frozen for up to five days while a prosecutor investigates the suspicious activity. Switzerland cooperates with the United States to trace and seize assets, and has shared a large amount of funds seized with the U.S. Government (USG) and other governments. The Government of Switzerland (GOS) has worked closely with the USG on numerous money laundering cases. Swiss legislation permits "spontaneous transmittal," a process allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. Eight percent of the 1,693 foreign judicial assistance requests originated from the U.S. However, Swiss privacy laws make it extremely difficult for bank officials and Swiss police to divulge financial crime information to U.S. authorities absent a Mutual Legal Assistance Treaty (MLAT) request or Letters Rogatory.

Since September 11, 2001, Swiss authorities regularly alert banks and nonbank financial intermediaries to check their records and accounts against lists of persons and entities with links to terrorism. The accounts of these individuals and entities are to be reported to the Ministry of Justice as suspicious transactions. Based on the "state security" clause of the Swiss Constitution, the authorities have ordered banks and other financial institutions to freeze the assets of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

Along with the U.S. and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of individuals and entities connected with international terrorism or its financing. Swiss authorities have thus far blocked about 48 accounts totaling SFr. 25.5 million (approximately U.S. \$20,648,360) from individuals or companies linked to individuals or entities listed pursuant to relevant UN resolutions. The Swiss Attorney General also separately froze 41 accounts representing about SFr. 25 million (approximately U.S. \$22,943,800) on the grounds that they were related to terrorist financing, but the extent to which these funds overlap with the UN consolidated list has yet to be determined.

Switzerland has ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Switzerland is a party to the 1988 UN Drug Convention. Switzerland ratified the UN Convention against Transnational Organized Crime on October 27, 2006. Swiss ratification of the UN Convention against Corruption is still pending.

Swiss authorities cooperate with counterpart bodies from other countries. Switzerland has a mutual legal assistance treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for supervisory purposes. Switzerland is a member of the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision, and its FIU is a member of the Egmont Group.

The Government of Switzerland hopes to correct the country's image as a haven for illicit banking services. The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or exceeds that of other countries. The primary interest of the Swiss system is to avert bad risks by countering them at the account-opening phase, where due diligence and know-your-customer procedures address the issues, rather than relying on an early-warning system on all filed transactions. The GOS believes that because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in some other countries. At the same time, 82 percent of the STRs that are filed lead to the opening of criminal investigations. While generally positive, Switzerland's FATF mutual evaluation report nonetheless identified weaknesses in the Swiss anti-money laundering and counter-terrorist financing regime, including problems with correspondent banking and the identification of beneficial owners. Per FATF Special Recommendation IX, the GOS should implement cross-border currency reporting requirements. Switzerland should also put forward effective AML legislation and rules that monitor and regulate money service businesses.

Syria

Syria is not an important regional or offshore financial center, due primarily to its still underdeveloped private banking sector and the fact that the Syrian pound is not a fully convertible currency. Despite rapid growth in the banking sector since 2004, industry experts estimate that only eight percent of Syria's population of nearly 20 million people actually uses banking services. Consequently, some 70 percent of all business transactions are still conducted in cash. Additionally, there continue to be significant money laundering and terrorist financing vulnerabilities in Syria's financial and nonbank financial sectors that have not been addressed by necessary legislation or other government action. Syria's black market moneychangers are not adequately regulated, and the country's borders remain porous. Regional hawala networks are intertwined with smuggling and trade-based money laundering and raise significant concerns, including involvement in the financing of terrorism. The most obvious indigenous money laundering threat involves Syria's political and business elite, whose corruption and extra-legal activities continue unabated. The U.S. Department of State has designated Syria as a State Sponsor of Terrorism.

The Syrian banking sector is dominated by the Commercial Bank of Syria (CBS), which holds approximately 75 percent of all deposits and controls most of the country's foreign currency reserves. With growing competition from private banks, CBS and the country's four other specialized public banks—the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank—have begun offering a broader range of retail services to private customers. However, these state-owned banks still retain a monopoly on all government banking business, and account for some 80 percent of all bank branches nationwide. Furthermore, as a state-owned bank, CBS has no bottom-line incentive to stop financing Syria's many poor-performing public enterprises.

In May 2004, the U.S. Department of Treasury designated CBS, along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of “primary money laundering concern,” pursuant to Section 311 of the USA PATRIOT Act. This designation resulted from information that CBS has been used by terrorists or persons associated with terrorist organizations, as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil, and continued concerns that CBS is vulnerable to exploitation by criminal and/or terrorist enterprises. In April 2006, Treasury promulgated a final rule, based on the 2004 designation, prohibiting U.S. financial institutions from maintaining or opening correspondent accounts with CBS or its Syrian Lebanese Commercial Bank subsidiary.

The Syrian Arab Republic Government (GOS) began taking steps to develop a private banking sector in April 2001, with Law No. 28, which legalized private banking, and Law No. 29, which established rules on bank secrecy. Under Law No. 28, subsidiary branches of private foreign banks are required to have 51 percent Syrian ownership to be licensed in Syria. Bank of Syria and Overseas, a subsidiary of Lebanon’s BLOM Bank, was the first private bank to open in Syria in January 2004. There are now seven private banks in Syria, including Bank of Syria and Overseas (BSOM), Banque BEMO Saudi Fransi, the International Bank for Trade and Finance, Bank Audi, Arab Bank, Byblos Bank, and Syria Gulf Bank. Three more private banks, the Bank of Jordan, Fransa Bank and Qatar National Bank have obtained the necessary licenses and are expected to begin operations in Syria in 2008. A new law was enacted in May 2005 that allows for the establishment of Islamic banks and the first such bank, al-Sham Islamic Bank, began operations in August 2007. Shortly thereafter, Syria International Islamic Bank (IIB) opened its doors in September. Al-Baraka Islamic Bank was also officially licensed in 2007 and is expected to begin operations in early 2008.

By mid-2007, the Syrian banking sector reported assets totaling U.S. \$29.5 billion and held deposits totaling \$17.2 billion. Syrian banks are playing an increasing role in providing the business sector with foreign currency to finance imports and as a source of credit for businesses and individuals. However, the sector’s development is hampered by the continuing lack of human expertise in finance, insufficient automation and communication infrastructure, regulations that limit Syrian banks’ ability to make money on their liquidity, and restrictions on foreign currency transactions.

Syria’s free trade zones also may provide an easy entry or transit point for the proceeds of criminal activities. There are seven free zones in Syria, serviced mostly by subsidiaries of Lebanese banks, including BLOM (Bank du Liban et d’Autre Mer), BEMO (Banque Europeenne Pour le Moyen-Orient Sal), BBAC (Bank of Beirut and Arab Countries), Bank Societee Generale, Fransa Bank, SBA (Societee du Banks Arabe) and Basra International Bank. Four additional public free zones are planned to be established in Homs, Dayr al Zur, Idleb, and the Port of Tartous. The Al-Ya’rubiyeh free zone in al-Hasakeh province, near the northeastern Syrian-Iraqi border, is scheduled to be opened in early 2008.

In recent years, both China and Iran announced plans to build free zones in Syria, although Iran later dropped this idea in favor of pursuing a regular Free Trade Agreement with Syria. China’s free zone in Adra, however, is on-schedule to provide roughly 200 Chinese companies with a regional gateway for their goods. Recently, a Syrian investor, in cooperation with partners from the Gulf, obtained preliminary approval for the establishment of a private free zone near the al-Tanf border crossing with Iraq. The volume of goods entering the free zones is estimated to be in the billions of dollars and is growing, especially with increasing demand for automobiles and automotive parts, which enter the zones free of customs tariffs before being imported into Syria. While all industries and financial institutions in the free zones must be registered with the General Organization for Free Zones, which is part of the Ministry of Economy and Trade, the Syrian General Directorate of Customs continues to lack strong procedures to check country of origin certification or the resources to adequately monitor goods that enter Syria through the zones. There are also continuing reports of Syrians using the free zones to import arms and other goods into Syria in violation of USG sanctions under the Syrian Accountability and Lebanese Sovereignty Act.

Legislation approved in the last few years provides the Central Bank of Syria with new authority to supervise the banking sector and investigate financial crimes. In September 2003, the GOS passed Decree 59; this criminalized money laundering and created an Anti-Money Laundering Commission (Commission) in May 2004. In response to international pressure to improve its anti-money laundering and counter-terrorist financing (AML/CTF) regulations, the GOS passed Decree 33 in May 2005, which strengthened the Commission and empowered it to act as a Financial Intelligence Unit (FIU). The Decree finalized the Commission's composition to include the Governor of the Central Bank, a Supreme Court Judge, the Deputy Minister of Finance, the Deputy Governor for Banking Affairs, and the GOS's Legal Advisor, and will include the Chairman of the Syrian Stock Market once the market is operational.

Under Decree 33, all banks and nonbank financial institutions are required to file reports with the Commission for transactions over \$10,000, as well as Suspicious Transaction Reports (STRs) regardless of amount. They are also required to use "know your customer" (KYC) procedures to follow up on their customers every three years and maintain records on closed accounts for five years. The chairmen of Syria's private banks continue to report that they are employing internationally recognized KYC procedures to screen transactions and also employ their own investigators to check suspicious accounts. Nonbank financial institutions must also file STRs with the Commission, but many of them continue to be unfamiliar with the requirements of the law. The Commission has organized workshops for these institutions over the past two years, but more time is needed for the information to penetrate the market.

Once a STR has been filed, the Commission has the authority to conduct an investigation, waive bank secrecy on specific accounts to gather additional information, share information with the police and judicial authorities, and direct the police to carry out a criminal investigation. In addition, Decree 33 empowers the Governor of the Central Bank, who is the chairman of the Commission, to share information and sign Memoranda of Understanding (MOUs) with foreign FIUs. In November 2005, the Prime Minister announced that the Commission had completed an internal reorganization, creating four specialized units to: oversee financial investigations; share information with other GOS entities including customs, police and the judiciary; produce AML/CTF guidelines and verify their implementation; and develop a financial crimes database.

Decree 33 provides the Commission with a relatively broad definition of what constitutes a crime of money laundering, but one that does not fully meet international standards. The definition includes acts that attempt to conceal the proceeds of criminal activities, the act of knowingly helping a criminal launder funds, and the possession of money or property that resulted from the laundering of criminal proceeds. In addition, the law specifically lists thirteen crimes that are covered under the AML legislation, including narcotics offenses, fraud, and the theft of material for weapons of mass destruction. It is unclear whether terrorist financing is a predicate offense for money laundering or otherwise punishable under Decree 33.

While a STR is being investigated, the Commission can freeze accounts of suspected money launderers for a nonrenewable period of up to eighteen days. The law also stipulates the sanctions for convicted money launderers, including a three to six-year jail sentence and a fine that is equal to or double the amount of money laundered. Further, the law allows the GOS to confiscate the money and assets of the convicted money launderer. The Commission circulates among its private and public banks the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list. has taken action to freeze the assets of designated individuals, but has not frozen the assets of any Syrian citizens in 2007.

In 2007, the Commission investigated 130 suspicious transaction cases, 15 of which were forwarded by foreign countries, including Qatar, Croatia and Ukraine. Eleven of these cases were referred to the criminal court system for prosecution. Over the past two years, the Commission investigated 263 cases

and referred 34 of them to the criminal court system. At the end of 2007, all criminal cases are pending, and there have been no convictions. Most Syrian judges are not yet familiar with the evidentiary requirements of the law. Furthermore, the slow pace of the Syrian legal system and political sensitivities delay quick adjudication of these issues. The Commission itself continues to be seriously hampered by human resource constraints, although it has increased its staff from six in 2005 to ten in 2007, and hopes to expand to 30 by the end of 2008. However, the lack of expertise further undermined by a lack of political will continues to impede effective implementation of existing AML/CTF regulations.

The GOS has not updated its laws regarding charitable organizations to include strong AML/CTF language. A promised updated draft law is still pending. The GOS decided at the end of 2004 to restrict charitable organizations to only distributing nonfinancial assistance, but the current laws do not require organizations to submit detailed financial information or information on their donors. While the Commission says that it is seeking to increase cooperation with the Ministry of Social Affairs and Labor, which is supposed to approve all charitable transactions, this remains a largely unregulated area.

Although Decree 33 provides the Central Bank with the legal basis to combat money laundering, most Syrians still do not maintain bank accounts or use checks, credit cards, or ATM machines. The Syrian economy remains primarily cash-based, and Syrians use moneychangers, some of whom also act as hawaladars, for many financial transactions. Estimates of the volume of business conducted in the black market by Syrian moneychangers range between \$15-70 million per day. Even the GOS admits that it does not have visibility into the amount of money that currently is in circulation. The GOS has begun issuing new regulations to entice people to use the banking sector, including offering high interest certificates of deposit and allowing Syrians to access more foreign currency from banks when they are traveling abroad. The GOS also passed a Moneychangers Law in 2006 to try to regulate the sector, requiring moneychangers to receive a license. However, it is unlikely that black market currency transactions will enter the formal sector because the GOS has still not offered adequate incentives; there is a 25 percent tax on these transactions, inadequate enforcement mechanisms, and continuing restrictions on foreign currency transfers. Although moneychangers had until the end of 2006 to license their operations, to date, only nine moneychangers applied for licensing and just two money exchange offices have begun operating legally. The Commission does have the authority to monitor the sector under Decree 33, but the GOS has not yet begun investigating illegal money-changing operations. Consequently, hawaladars in Syria's black market remain a source of concern for money laundering and terrorist financing.

While the GOS maintains strict controls on the amount of money that individuals can take with them out of the country, there is a high incidence of cash smuggling across the Lebanese, Iraqi, and Jordanian borders. Most of the smuggling involves the Syrian pound, as a market for Syrian currency exists among expatriate workers and tourists in Lebanon, Jordan, and the Gulf countries. U.S. dollars are also commonly smuggled in the region. Some of the smuggling may involve the proceeds of narcotics and other criminal activity. In addition to cash smuggling, there also is a high rate of commodity smuggling out of Syria, particularly of diesel fuel, prompted by individuals buying diesel domestically at the low subsidized rate and selling it for much higher prices in neighboring countries. There are reports that some smuggling is occurring with the knowledge of or perhaps even under the authority of the Syrian security services.

The General Directorate of Customs lacks the necessary staff and financial resources to effectively handle the problem of smuggling. And while it has started to enact some limited reforms, including the computerization of border outposts and government agencies, problems of information-sharing remain. In September 2006, the Minister of Finance issued a decision stipulating the establishment of a unit specializing at combating money laundering and terrorist financing in the General Directorate of Customs. Additionally, Customs currently lacks the infrastructure to effectively monitor or control

even the legitimate movement of currency across its borders. The Commission and Customs have reportedly implemented a form asking individuals to voluntarily declare currency when entering or exiting the country, although consistency of implementation and any action resulting from enforcement remain unknown.

Syria is one of the fourteen founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. In 2006, Syria underwent a mutual evaluation by its peers in MENAFATF and the released evaluation report found Syria to be fully compliant with five of the 49 recommendations, largely compliant on eight, partially compliant on 26 and noncompliant on eight, although two of those eight recommendations were not applicable to Syria. In 2007, the Syrian FIU became a fully accepted member of the Egmont Group.

Syria is a party to the 1988 UN Drug Convention. In April 2005, it became a party to the International Convention on the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Syria has signed, but not ratified the UN Convention against Corruption. Syria is ranked 138 out of 180 countries on Transparency International's 2007 Corruption Perception Index.

While Syria has made modest progress in implementing AML/CTF regulations that govern its formal financial sector, the continuing lack of transparency of the state-owned banks and their vulnerability to political influence reveals the absence of political will to address AML/CTF in the largest part of the banking sector. In addition, nonbank financial institutions and the black market will continue to be vulnerable to money laundering and terrorist financiers. To build confidence in Syria's intentions, the Central Bank should be granted independence and supervisory authority over the entire sector. Additionally, Syria should continue to modify its AML/CTF legislation and enabling regulations so that they adhere to global standards. The General Directorate of Customs, the Central Bank, and the judicial system in particular continue to lack the resources and the political will to effectively implement AML/CTF measures. Although the GOS has stated its intention to create the technical foundation through which different government agencies could share information about financial crimes, this does not exist. In addition, it remains doubtful that the GOS has the political will to punish terrorist financing, by classifying what it sees as legitimate resistance groups as terrorist organizations, or to address the corruption that exists at the highest levels of government and business. All of these issues remain obstacles to developing a comprehensive and effective AML/CTF regime in Syria. The GOS should become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it susceptible to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes, such as narcotics trafficking, trade fraud, and smuggling. There has traditionally been a significant volume of informal financial activity through unregulated nonbank channels, but in recent years Taiwan has taken steps to shift much of this activity into official, regulated financial channels. Most illegal or unregulated financial activities are related to tax evasion, fraud, or intellectual property violations. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes most commonly linked to SAR reporting include financial crimes, corruption, and other general crimes.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997, which was amended in 2003 and in 2007. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit (FIU), the Money Laundering Prevention Center (MLPC).

The MLPC, a law enforcement-style FIU, is located within the Ministry of Justice Investigation Bureau (MJIB). The FIU is tasked to receive, analyze, and disseminate suspicious transaction reports, currency transaction reports and cross-border currency movement declaration reports. The MLPC also assists other law enforcement authorities to investigate money laundering and terrorist financing cases. MLPC staff has law enforcement status.

The 2003 amendment expanded the list of predicate crimes for money laundering, widened the range of institutions subject to suspicious transaction reporting, and mandated compulsory reporting to the MLPC of significant currency transactions in excess of New Taiwan dollars (NT \$) 1 million (approximately U.S. \$30,980). As of November 2007, the MLPC received 1,065,879 currency transaction reports and in 2006 it received 1,089,768. The amendments further expanded the scope of reporting entities beyond traditional financial institutions to include: automobile dealers, jewelers, boat and aviation dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers.

In July 2007, the MLCA was amended to expand its coverage to include a new agricultural bank, trust companies, and newly licensed currency exchanges as well as hotels, jewelry stores, postal offices, temples, and bus/railway stations. The list of predicate offenses was expanded to include offenses against the Public Procurement Law, Bills Finance Management Law, Insurance Law, Financial Holding Company Law, Trust Law, Credit Cooperative Association Law, and Agriculture Financing Law. The number of agencies with money laundering responsibilities was expanded from the Ministry of Justice, Ministry of Transportation and Communication, and Ministry of Finance to include also the Financial Supervisory Commission (established in July 2004), Ministry of Economic Affairs, Council of Agriculture (supervising a new agriculture bank and the credit departments of farmers' and fisherman's associations), and Taiwan's Central Bank (monitoring currency exchanges). The amended law also authorized Taiwan agencies to share information obtained from the MLCA with law enforcement agencies in countries that have signed a mutual legal assistance agreement (MLAA) with Taiwan and on a reciprocal basis with other countries.

Taiwan set up a single financial regulator, the Financial Supervisory Commission (FSC) on July 1, 2004. The FSC consolidates the functions of regulatory monitoring for the banking, securities, futures and insurance industries, and also conducts financial examinations across these sectors. In mid-December 2005, the FSC began an incentive program for the public to provide information on financial crimes. The reward for information on a financial case with fines of NT \$10 million (approximately U.S. \$309,000) or at least a one-year sentence is up to NT \$500,000 (approximately U.S. \$15,500). The reward for information on a case with a fine of between NT \$2 and \$10 million (approximately U.S. \$61,500 and \$308,000) or less than a one-year sentence is up to NT \$200,000 (approximately U.S. \$6,200).

Two new articles added to the 2003 amendments to the MLCA grant prosecutors and judges the power to freeze assets related to suspicious transactions and give law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. The 2007 amendment to the MLCA permits the freezing of proceeds of money laundering for up to one year. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. The time limit for reporting cash transactions of over NT \$1 million is five business days. Banks are barred from informing customers that a suspicious transaction report has been filed. Reports of suspicious transactions must be submitted to the MLPC within 10 business days. In 2006, the MLPC received 1,281 suspicious transaction reports and 689 of them resulted in prosecutions. As of November 2007, the MLPC received 2,953 reports. Thirty of them involved an amount exceeding NT \$5 million (approximately U.S. \$154,600), which resulted in prosecutions based on the MCLA. Of these 30 cases, 19 relate to financial crimes, four to corruption, one to narcotics, and six to other miscellaneous crimes.

Institutions are also required to maintain records necessary to reconstruct significant transactions. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MLPC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance issued instructions requiring banks to demand two types of identification and to retain photocopies of the identification cards when bank accounts are opened on behalf of a third party, to prove the true identity of the account holder. Individual bankers can be fined NT \$200,000 to \$1 million (approximately U.S. \$6,200 to \$30,900) for not following the provisions of the MLPA. Starting in August 2006, the Financial Supervisory Commission required banking institutions to collect, verify and store information about any banking customer that makes any single cash or electronic remittance above NT \$30,000 (approximately \$927). The requirement was adopted in response to suggestions submitted to Taiwan in 2004 by the FATF.

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the disclosure regulations from the Central Bank, the Banking Bureau of the Financial Supervisory Commission, and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and Internet gambling sites are illegal. According to the Central Bank, as of September 2007, Taiwan hosted 32 local branches of foreign banks, two trust and investment companies, and 65 offshore banking units.

On January 5, 2006, legislation was ratified to allow expansion of offshore banking unit (OBU) operations to the same scope as Domestic Business Units (DBU). This was done to assist China-based Taiwan businesspeople in financing their business operations. DBUs engaging in cross-strait financial business must follow the regulations of the “Act Governing Relations between Peoples of the Taiwan Area and the Mainland Area” and “Regulations Governing Approval of Banks to Engage in Financial Activities between the Taiwan Area and the Mainland Area.” The Competent Authority, as referred to in these Regulations, is the Financial Supervisory Commission (FSC).

Taiwan prosecuted 689 cases involving money laundering in 2006, compared with 947 cases involving financial crimes during the same period of 2005. Among the 689 cases, 631 involved unregistered stock trading, credit card theft, currency counterfeiting or fraud. Among the 58 other money laundering cases, 11 were corruption-related and one was drug-related. In July 2007, the MCLA was amended so that only cases involving amounts exceeding NT \$5 million (U.S. \$154,578) were covered under the MLCA, while the rest were handled in accordance with other laws. Figures for the full year are not available yet, but the number of MLCA-based prosecution cases in the first 11 months dropped to 30. Using the most current figures available, between January and October 2007, the number of drug-related investigations reached 73,411, an increase of 13.4 percent when compared to the same period in 2006. Only 10 percent of these cases were related to drug trafficking. The number of subjects investigated in 2007 increased 10.9 percent to 71,202 from January-October 2006. The number of indicted subjects grew 36 percent to 31,614 from January-October 2007 and the number of subjects cleared further declined 5.6 percent to 16,657.

To comply with Financial Action Task Force (FATF) Special Recommendation Nine on bulk cash smuggling, the July 2007 legislation required individuals to report currency transported into or out of Taiwan in excess of NT \$60,000 (approximately U.S. \$1,850), U.S. \$10,000 in foreign currency, 20,000 Chinese Yuan (approximately U.S. \$2,700), or gold worth more than U.S. \$20,000. When foreign currency in excess of NT \$500,000 (approximately U.S. \$15,400) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign currency when the amount exceeds U.S. \$5 million for an individual resident and U.S. \$50 million for a corporate entity. Starting August 1, 2006, those who transfer funds over NT \$30,000 (approximately U.S. \$900) at any bank in Taiwan must

produce a photo ID, and the bank must record the name, ID number and telephone number of the client.

The authorities on Taiwan are actively involved in countering the financing of terrorism. A new “Counter-Terrorism Action Law” (CTAL) has been under review by the Legislative Yuan since 2003. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB, and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order.

Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the proposed CTAL, unless the assets could be identified as belonging to victims of the crimes. Under the MLCA Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement.

The Banking Bureau of the FSC circulates the names of individuals and entities included on the UN 1267 Sanctions Committee’s consolidated list, as well as names designated by the U.S. Treasury, to all domestic and foreign financial institutions and relevant government agencies. Banks are required to file a report on cash remittances if either of the parties involved are on a terrorist list. Although, as noted above, Taiwan does not yet have the authority to confiscate the assets, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities in Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers, after obtaining approval from the Central Bank, are authorized to use banks to remit income earned by foreign workers to their home countries. These brokers may not start the remittance services before they obtain the guaranty of their correspondent banks. They are required to sign and retain a standard remittance service contract with foreign workers and establish remittance records for each contracting foreign worker. There were 25 foreign labor employment brokers as of December 2007. If brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law. It is illegal for retail outlets to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance, and/or a fine equal to the remittance amount.

In April 2007, the Ministry of Justice Investigation Bureau (MJIB) uncovered a 13-office network engaged in cross-Strait underground remittances and money laundering. The network’s accounting records showed that cross-Strait underground remittances through the network exceeded NT \$2.1 billion (U.S. \$63 million). The MJIB arrested eight persons. Over the past five years, the MJIB has uncovered 43 cross-Strait underground remittance channels involving capital flows totaling NT \$136.2 billion (U.S. \$4.2 billion).

Authorities in Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism. Such organizations are required to register with the government and, like any other individual or corporate entity, are checked against list of names designated by the United Nations or the U.S. Treasury as being involved in terrorist financing activities. The Ministry of Interior (MOI) is in charge of overseeing foundations and charities. In 2004 and in 2006, the MOI assigned public accountants to audit the financial management of nationwide foundations.

Article 3 of Taiwan’s Free Trade Zone Establishment and Management Act defines a Free Trade Zone (FTZ) as a controlled district of an international airport or an international seaport approved by the Executive Yuan. The FTZ coordination committee, formed by the Executive Yuan, has the

responsibility of reviewing and examining the development policy of the FTZ, the demarcation and designation of FTZs, and inter-FTZ coordination.

There are five FTZs in Taiwan, all of which have opened since 2004, including the Taipei Free Trade Zone, the Taichung Free Trade Zone, the Keelung Free Trade Zone, the Kaohsiung Free Trade Zone, and the Taoyuan Air Cargo Free Trade Zone. These FTZs were designated with different functions, so that Keelung and Taipei FTZs focus on international logistics; Taoyuan FTZ on adding value to high value added industries; Taichung FTZ on warehousing, transshipment and processing of cargo; and Kaohsiung FTZ on mature industrial clusters. According to the Center for Economic Deregulation and Innovation (CEDI) under the Council for Economic Planning & Development, as of November 2007 there were 17 shipping and logistics companies listed in the Kaohsiung Free Trade Zone, 19 logistics companies in Taichung Free Trade Zone, 11 logistics and shipping companies in Keelung Free Trade Zone, one logistics company in Taipei Free Trade Zone, and 81 manufacturers and enterprises in Taoyuan Air Cargo Free Trade Zone. Shipments through these FTZs in the first ten months of 2007 was valued at NTD 43.7 billion (\$1.3 billion), equivalent to 0.3 percent of Taiwan's two-way trade in the same period. There is no indication that FTZs in Taiwan are being used in trade-based money laundering schemes or by the financiers of terrorism. According to Article 14 of the Free Trade Establishment and Management Act, any enterprise applying to operate within an FTZ shall apply to the management authorities of the particular FTZ by submitting a business operation plan, the written operational procedures for good control, customs clearance, and accounting operations, together with relevant required documents. Financial institutions may apply to establish a branch office inside the FTZ and conduct foreign exchange business, in accordance with the Banking Law of the ROC, Securities and Exchange Law, Statute Governing Foreign Exchange, and the Central Bank of China Act.

According to Taiwan's Banking Law and Securities Trading Law, in order for a financial institution to conduct foreign currency operations, Taiwan's Central Bank must first grant approval. The financial institution must then submit an application to port authorities to establish an offshore banking unit (OBU) in the free-trade zone. No financial entity has yet applied to establish such an OBU in any of the five free trade zones. An offshore banking unit may operate a related business under the Offshore Banking Act, but cannot conduct any domestic financial, economic, or commercial transaction in New Taiwan Dollars.

Taiwan has promulgated drug-related asset seizure and forfeiture regulations that provide—in accordance with treaties or international agreements—Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions, or international parties that provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. The Ministry of Justice distributes other seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for Taiwan and U.S. law enforcement agencies to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities in Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and in 2005, was elected to the APG steering committee. In 2007, Taiwan underwent its second round mutual evaluation by the APG.

The MLPC is a member of the Egmont Group of financial intelligence units. The Investigation Bureau of the Ministry of Justice has actively engaged in international cooperation, and the number of cooperation cases in the first 11 months of 2007 reached 74. The MOJ has signed mutual legal assistance memoranda with four jurisdictions.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should endeavor to pass the proposed Counter-Terrorism Action Law to better address terrorist financing issues. The authorities on Taiwan should investigate underground finance and its links to trade and also enact legislation regarding alternate remittance systems.

Tanzania

While not an important regional financial center, Tanzania is vulnerable to money laundering and has weaknesses in its anti-money laundering/counter-terrorist financing (AML/CTF) regime, specifically in its financial institutions and law enforcement capabilities. However, with the enactment of the Anti-Money Laundering (AML) Act, 2006 and the creation of a financial intelligence unit (FIU), the Government of Tanzania (GOT) is improving its capability to track and prosecute money laundering. Money laundering is more likely to occur in the informal nonbank financial sector, as opposed to the formal sector, which is largely undeveloped. Real estate and used car businesses appear to be vulnerable trade industries involved in money laundering. Front companies are used to launder funds including hawaladars and bureaux de change, especially on the island of Zanzibar, where few federal regulations apply. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling. The likely sources of illicit funds are from Asia and the Middle East and, to a lesser extent, Europe. Such transactions rarely include significant amounts of U.S. currency. There are no indications Tanzania's two free trade zones are being used in trade-based money laundering schemes or by financiers of terrorism.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It requires all financial institutions to inform the government each quarter in a calendar year of any assets or transactions that may be associated with a terrorist group. The implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The Bank of Tanzania (BOT) circulates to Tanzanian financial institutions the names of suspected terrorists and terrorist organizations on the United Nations Security Council Resolution (UNSCR) 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. In 2004, the Government of Tanzania took action against one charitable organization on the list by closing its offices and deporting its foreign directors. However, it is not clear whether Tanzania has the investigative capacity to identify and seize related assets. Tanzania has cooperated with the U.S. in investigating and combating terrorism and exchanges counterterrorism information. There are no specific laws in place allowing Tanzania to exchange records with the U.S. on narcotics transactions or narcotics-related money laundering.

Tanzania made progress in 2007 with its anti-money laundering legislation. The national multi-disciplinary committee, established with the help of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), finalized the AML bill in 2005 after gaining input from a wide range of stakeholders. The Anti-Money Laundering Act, which creates a financial intelligence unit as an extra-ministerial department of the Ministry of Finance, was passed by the Parliament in December 2006 and signed into law in July 2007. The AML regulations implementing the Act were published in September 2007. The AML Act empowers the FIU to receive and share information with foreign FIUs and other comparable bodies. At present, the FIU has a small core staff—a Commissioner, an analyst,

and an information technology expert. Current plans call for the recruitment of three additional staff members. The FIU has not yet set up its office and has not yet begun the analysis of suspicious transactions. It is working toward building capacity to become operational, and has applied for membership in the Egmont Group.

The AML Act criminalizes cash smuggling in and out of Tanzania. The AML Act and regulations require all “reporting persons”—banks and financial institutions, cash dealers, accountants, real estate agents, dealers in precious stones, customs officers, auctioneers, and legal professionals handling real estate or funds—to obtain specific information from citizen and noncitizen customers, maintaining specific identification procedures, and to report suspicious and unusual transactions to the FIU within 24 hours. The AML Act governs all serious crimes, including narcotics and terrorism. The FIU is developing a sensitization and outreach program to ensure that financial and nonfinancial institutions are aware of their reporting obligations under the AML Act.

The GOT is a party to the 1988 UN Drug Convention; the UN International Convention for the Suppression of the Financing of Terrorism; the UN Convention Against Corruption; and the UN Convention against Transnational Organized Crime. Tanzania is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). The Government of Tanzania has detailed personnel to the ESAAMLG Secretariat. In 2007, Tanzania was listed 94 out of 179 countries in Transparency International’s Corruption Perceptions Index.

Tanzania has made many improvements in its compliance with international AML standards. The GOT should focus on the practical implementation of its new AML Act, including dedicating the resources necessary to build an effective FIU. The FIU should work towards attaining international standards and membership in the Egmont Group.

Thailand

Thailand has introduced a number of measures in recent years to strengthen its AML/CTF framework. Illicit proceeds are generated from drug trafficking, illegal gambling, theft, corruption, prostitution, human trafficking, illegal logging, production and distribution of counterfeit consumer goods, production and sale of counterfeit travel documents, and from crime in bordering countries. Thailand remains a transit point for heroin en route to the international drug markets from Burma and Laos, and a drug money laundering center for transnational organized crime groups in Thailand. Authorities believe Thailand’s major narcotics problem now is the trafficking of large quantities of methamphetamine produced in Burma. The illegal economy in Thailand is estimated as much as 13 percent of gross domestic product (GDP) and money laundering predicate offenses are estimated to generate illicit proceeds as much as five percent of Thailand’s GDP. The widespread use of cash and a large informal sector provide many avenues for illicit proceeds to be laundered in Thailand.

Thailand’s 1999 anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 criminalizes money laundering for the following predicate offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, public fraud, blackmail, and terrorist activity. On August 11, 2003, as permitted by the Thai constitution, the Royal Thai Government (RTG) issued two Emergency Decrees to enact measures related to terrorist financing that had been under consideration by the Executive Branch and Parliament for more than a year and a half. The first of these Decrees amended Section 135 of the Penal Code to establish terrorism as a criminal offense. The second Decree amended Section 3 of the AMLA to add the newly established offense of terrorism and terrorist financing as an eighth predicate offense for money laundering. The Decrees took effect when they were published. Parliament endorsed their status as legal acts in April 2004. No cases of terrorist financing have been prosecuted.

The current list of predicate offenses in the AMLA does not meet international best practices standards consistent with the first and second recommendations of the Financial Action Task Force (FATF) 40 Recommendations, which apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of “property involved in an offense” in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense.

The AMLA created the Anti-Money Laundering Office (AMLO). Among other functions it serves as Thailand’s financial intelligence unit (FIU), which became fully operational in 2001. When first established, AMLO reported directly to the Prime Minister. In October 2002, pursuant to a reorganization of the executive branch following criticisms that AMLO had been politicized, AMLO was designated as an independent agency under the Minister of Justice.

AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. In addition, AMLO is responsible for investigating money laundering cases for civil forfeiture and for the custody, management, and disposal of seized and forfeited property. AMLO is also tasked with providing training to the public and private sectors concerning the AMLA. The law also created the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Anti-Money Laundering Board, which is comprised of ministerial-level officials and agency heads and serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose relevant ministerial regulations.

AMLO, the Bank of Thailand, the Securities and Exchange Commission, and the Department of Special Investigation (DSI) are responsible for investigating financial crimes. During the 2007 fiscal year, AMLO forwarded 83 cases for civil asset forfeiture to the Attorney General’s office for prosecution totaling 309 million baht in Thai currency (approximately U.S. \$10.5 million); fifteen other cases remain under investigation. AMLO has a memorandum of understanding with the Royal Thai Customs, which shares information and evidence of smuggling and customs evasion involving goods or cash exceeding one million baht (approximately U.S. \$34,000) with AMLO. In criminal narcotics cases, the forfeiture and seizure of assets is governed by the 1991 Act on Measures for the Suppression of Offenders in an Offense relating to Narcotics (Assets Forfeiture Law). The Assets Examination Committee, which is separate from AMLO and was created by the post coup government to deal with corruption, has filed 1,865 cases with assets valued at 1.64 billion baht (approximately U.S. \$56.6 million) and 1,644 cases are on trial.

The Ministry of Justice also houses a criminal investigative agency, the Department of Special Investigations (DSI), which is separate from the Royal Thai Police (RTP). DSI has responsibility for investigating the criminal offense of money laundering (as distinct from civil asset forfeiture actions carried out by AMLO) and for several of the money laundering predicates defined by the AMLA, including terrorism. The DSI, AMLO, and the RTP all have authority to identify, freeze, and/or forfeit terrorist finance-related assets.

Article 13 of the Anti-Money Laundering Act, B.E. 2542 requires financial institutions to submit three categories of cash transactions. For example, transactions that are worth two million baht (approximately U.S. \$68,300) or more; transactions involving assets worth five million baht (approximately U.S. \$170,000) or more; and suspicious transactions, on reasonable grounds, must be reported to the financial intelligence unit (FIU).

In addition to reporting large and suspicious transactions, financial institutions are also required to keep customer identification and specific transaction records for a period of five years from the date the account was closed, or from the date the transaction occurred, whichever is longer. Reporting individuals (banks and others) who cooperate with law enforcement entities are protected from liability. In January 2007, the Bank of Thailand issued notification to financial institutions (which

includes Thai and foreign commercial banks, finance companies, as well as assessment management companies) to adopt “know your customer” and customer due diligence procedures to comply with international standards and practices. The requirement was made effective immediately. However, there is no penalty for noncompliance. Thailand does not have stand-alone secrecy laws but the Commercial Bank Act B.E. 2505 (1962), regulated by Bank of Thailand, has a provision providing for bank secrecy to prevent disclosure of client financial information. However, AMLA overrides this provision, and financial institutions must disclose their client and ownership information to AMLO if requested.

The Bank of Thailand (BOT), Securities and Exchange Commission (SEC), and AMLO are empowered to supervise and examine financial institutions for compliance with anti-money laundering/counter-terrorist financing laws and regulations. Although the Bank of Thailand regulates financial institutions in Thailand, bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT’s auditing of a financial institution’s compliance with the AMLA or BOT regulations. Lacking power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. Legislation to eliminate the impediments is under review.

Anti-money laundering controls are also enforced by other Royal Thai Government (RTG) regulatory agencies, including the Board of Trade and the Department of Insurance. Financial institutions that are required to report suspicious activities are broadly defined by the AMLA as any business or juristic person undertaking banking or nonbanking business. The land registration offices are also required to report on any transaction involving property of five million baht or greater (approximately U.S. \$170,000), or a cash payment of two million baht or greater (approximately U.S. \$68,300) for the purchase of real property.

The Exchange Control Act of B.E. 2485 (1942), amended in 1984, states that foreign currencies can be brought into Thailand without limit. The Ministry of Finance issued a regulation, effective October 28, 2007, that requires any person who transports foreign currencies in or out of the country exceeding U.S. \$15,000, to declare such to the Customs office, which, in turn, reports the information directly to the Ministry. There is no restriction on the amount of Thai currency that may be brought into the country. However, absent authorization to exceed the limits, a person traveling to Thailand’s bordering countries including Vietnam is allowed to take out no more than 500,000 baht (approximately U.S. \$17,000) and to other countries no more than 50,000 baht (approximately U.S. \$1,700).

Thailand is not an offshore financial center nor does it host offshore banks, shell companies, or trusts. Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs) in March 1993. BIBFs may perform a number of financial and investment banking services, but can only raise funds offshore (through deposits and borrowing) for lending in Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. BIBFs are subject to the AMLA. However, in mid October 2006, the last BIBF license was returned to the Bank of Thailand due to the BOT’s “one presence” policy for all financial institutions. Some of these qualified “stand-alone” BIBFs have upgraded to either full branches or subsidiaries, while Thai commercial banks with BIBF licenses had to surrender their licenses to the BOT. Most BIBFs simply exited the market.

The Stock Exchange of Thailand (SET) requires securities dealers to have “know your customer” procedures; however, the SET does not check anti-money laundering compliance during its reviews. The Department of Insurance (DOI), under the Ministry of Commerce, is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly,

the Cooperative Promotion Department (CPD) is responsible for supervision of credit cooperatives, which are required under the Cooperatives Act to register with the CPD. Approximately 6,000 cooperatives are registered, with approximately 1,348 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives are engaged in deposit taking and providing loans to the members and are covered under the definition of a financial institution, but, as with the securities and insurance sectors, there are no anti-money laundering compliance mechanisms currently in place. These deficiencies have been recognized and are currently being addressed by the relevant government agencies.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons that act as solicitors for investors are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding two million baht (approximately U.S. \$68,300), and property transactions exceeding five million baht (approximately U.S. \$170,000), have been in place since October 2000. The AMLO Board is considering the issuance of an announcement or regulation to subject gold shops, jewelry stores, and car dealers to either mandatory transactional reporting requirements and/or suspicious transactions reporting requirements. Thailand has more than 6,000 gold shops and 1,000 gem traders that would be subject to these reporting requirements.

Thailand acknowledges the existence and use of alternative remittance systems (hawala, the Chinese underground banking system) that attempt to circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer, or to receive a transfer, that represents the proceeds of a specified criminal offense (including terrorism). Remittance and money transfer agents, including informal remittance businesses, require a license from the Ministry of Finance. Guidelines issued in August 2004 by the Ministry of Finance and the BOT prescribe that before they are granted a license, both money changers and money transfer agents are subject to onsite examination by the BOT, which also consults with AMLO on the applicant's criminal history and anti-money laundering prevention record. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office while remittance agents do not. Licensed agents are subject to monthly transaction reporting and a five-year record maintenance requirement for onsite inspections. At present, there are approximately 560 authorized moneychangers and 28 remittance agents. In 2004, the Bank of Thailand limited the maximum amount to \$5000 or equivalent for authorized moneychangers to sell foreign currencies and requires customers to present a passport or other traveling document. There are no limitations for buying currencies or no annual transaction volume. However, for remittance agents, the BOT limits the annual transaction volume for agents to U.S. \$60,000 for offices in the Bangkok area, and U.S. \$30,000 for offices located outside of Bangkok. Moneychangers frequently act as illegal remittance agents.

Money and property may be seized under Section 3 of the AMLA if derived from commission of a predicate offense, from aiding or abetting commission of a predicate offense, or if derived from the sale, distribution, or transfer of such money or asset. AMLO is responsible for tracing, freezing, and seizing assets. Instruments that are used to facilitate crime such as vehicles or farms (when not proceeds) cannot be forfeited under AMLA and are subject to seizure under the Criminal Asset Forfeiture Act of 1991, and unlike the AMLA, require a criminal conviction as a pre-requisite to a final forfeiture. The AMLA makes no provision for substitute seizures if authorities cannot prove a relationship between the asset and the predicate offense. Overall, the banking community in Thailand provides good cooperation to AMLO's efforts to trace funds and seize/freeze bank accounts.

The Bank of Thailand (BOT) does not have any regulations that give it explicit authorization to control charitable donations, but it is working with AMLO to monitor these transactions under the Exchange Control Act of 1942.

The Thai Prime Minister endorsed a cabinet decision in October 2007 to abolish an incentives system that went into effect three years earlier under the “Office of the Prime Minister’s Regulation on Payment of Incentives and Rewards in Proceedings against Assets under the Anti-Money Laundering Act.” Under this now largely defunct rewards system, AMLO investigators and their supervisors, as well as other investigative agencies were eligible to receive personal commissions on the property that they seized if it was ultimately forfeited. The United States, other countries, and international organizations, including UNODC, criticized this system on the grounds that it threatened the integrity of its AML regime and created a conflict of interest by giving law enforcement officers a direct financial stake in the outcome of forfeiture cases. The USG ceased providing technical assistance to the AMLO until the reward system was abolished,

Thailand is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed (December 2000), but not yet ratified, the UN Convention against Transnational Organized Crime. It has also signed (December 2003), but not yet ratified the UN Convention against Corruption.

The RTG has issued instructions to all authorities to comply with UNSCR 1267. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee’s consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions as possibly terrorist-related and has initiated investigations of possible terrorist activities using nongovernmental or nonprofit organizations as a front.

Thailand has Mutual Legal Assistance Treaties (MLATs) with 10 countries, including the United States. In 2006 Thailand signed the Treaty On Mutual Legal Assistance In Criminal Matters Among Like-Minded ASEAN Member Countries but has not yet ratified the agreement. AMLO has memoranda of understanding on money laundering cooperation with 31 other financial intelligence units and also exchanges information with FIUs with which it has not entered into an MOU, including the United States. Thailand cooperates with USG and other nations’ law enforcement authorities on a range of money laundering and illicit narcotics related investigations. AMLO responded to 87 requests for information from foreign FIUs in 2007. The AMLO joined the Egmont Group of financial intelligence units in June 2001.

Thailand became a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, in 1997. The most recent mutual evaluation of Thailand was conducted by the APG in 2007. The report noted that Thailand’s AML/CTF regime is “not fully in line with international standards and codes; there are weaknesses in the legal framework, the pursuit of money laundering cases, the coverage of institutions and in enforcement.”

AMLO has drafted amendments that will be proposed in early 2008 to deal with many of these deficiencies, including expanding the definition of property involved in an offense to include instrumentalities, creating an assets forfeiture fund, and restructuring AMLO. Additional amendments, approved by the Thai cabinet in February 2007 but still pending, would add additional predicate offenses under Section 5 of the AMLA, including environmental crimes, foreign exchange offenses, securities fraud, illegal gambling, firearms trafficking, bid-rigging, labor fraud, and customs and excise offenses.

The Government of Thailand should continue to implement AML/CTF programs that adhere to world standards, including expanding the number of predicate crimes to adhere to the minimum list of designated categories of offenses prescribed by FATF. Predicate offenses should include trafficking in humans and migrant smuggling, counterfeiting and intellectual property offenses, as well as the “structuring” of transactions. Per some of the major findings in the 2007 APG mutual evaluation, AML/CTF obligations should be extended to nonfinancial businesses and professions such as gold shops, jewelry stores and car dealers. The insurance and securities sectors should institute AML

compliance programs. Besides onsite consultation, AMLO should undertake audits of financial institutions to ensure compliance with requirements of AMLA and AMLO regulations. RTG authorities should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address the vulnerabilities presented by its alternative remittance systems. Customs and most law enforcement agencies need to provide more training on, and dedicate specialized staff to carry out, anti-money laundering and terrorist finance investigations, especially outside of Bangkok. Authorities should give higher priority to reducing the use of cash in Thailand and to encourage more activity in the formal sector to help reduce money laundering and terrorist finance risks. Authorities should place an emphasis on prosecuting money launderers; in 2005 and 2006 there were few money laundering prosecutions and no convictions. Thailand should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, narcotics trafficking organizations are only one source of the total funds laundered in Turkey. Other sources of laundered funds include smuggling, counterfeit goods, fraud, forgery, robbery, and kidnapping. Money laundering takes place in banks, nonbank financial institutions, and the underground economy. Money laundering methods in Turkey include: the cross-border smuggling of currency; bank transfers into and out of the country; trade fraud, and the purchase of high-value items such as real estate, gold, and luxury automobiles. It is thought that Turkish-based traffickers transfer money and sometimes gold via couriers, the underground banking system, and bank transfers to pay narcotics suppliers in Pakistan or Afghanistan. Funds are often transferred to accounts in the United Arab Emirates, Pakistan, and other Middle Eastern countries. A substantial percentage of money laundering that takes place in Turkey involves fraud and tax evasion. Informed observers estimate that as much as 40 to 50 percent of the economy is unregistered. In 2005, the Government of Turkey (GOT) passed a tax administration reform law, with the goal of improving tax collection. The GOT is working on additional reforms to combat the unregistered economy and move these businesses onto the tax rolls.

Turkey first criminalized money laundering in 1996. Under the law whoever commits a money laundering offense faces a sentence of two to five years in prison, and is subject to a fine of double the amount of the money laundered and asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), customer identification, and the maintenance of transaction records for five years.

In 2006, the GOT enacted additional anti-money laundering legislation, a new criminal law, and a new criminal procedures law. The new Criminal Law, which took effect in June 2005, broadly defines money laundering to include all predicate offenses for which the punishment is imprisonment for one year or more. Previously, Turkey's anti-money laundering law comprised a list of specific predicate offenses. A new Criminal Procedures Law also came into effect in June 2005.

Under a Ministry of Finance banking regulation circular all banks, including the Central Bank, securities companies, post office banks, and Islamic financial houses are required to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. The Ministry of Finance also mandates that a tax identity number be used in all financial transactions. The requirements are intended to increase the GOT's ability to track suspicious financial transactions. Turkey has a new law, which protects the identity of those who file suspicious transaction reports, and, as of October 2007, has helped to push suspicious transaction reports above 2,000. According to anti-money

laundering law Article 5, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes investigation Board (MASAK) or other authorities specified in Article 3 of the law. Individuals and corporate bodies from whom information and documents are requested may not withhold the requested items by claiming the protection provided by privacy provisions to avoid submitting the requested items. Despite the information collected for new accounts and transactions, customer due diligence (CDD) and other preventative measures have not been fully implemented and Turkey has failed to adopt a risk-based approach, as recommended by the Financial Action Task Force (FATF). There are no requirements for ongoing CDD and only limited requirements for the collection of beneficial ownership information. There is no requirement for financial institutions to exercise enhanced due diligence on business relationships or transactions with suspicious persons, including persons from or in countries which do not sufficiently apply FATF recommendations.

A new Banking Law was enacted in 2005 to strengthen bank supervision. The Banking Regulatory and Supervisory Agency (BRSA) conducts periodic anti-money laundering and compliance reviews under the authority delegated by MASAK. The number of STRs filed has been low, even taking into consideration the fact that many commercial transactions are conducted in cash. In 2006, 1140 STRs were filed. The upward trend continues as shown by the following results: in 2005, 352 STRs were filed; in 2004, 288 STRs were filed; and, in 2003, 177 STRs were filed.

Turkey does not have foreign exchange restrictions. With limited exceptions, banks and special finance institutions must inform authorities within 30 days about transfers abroad exceeding U.S. \$50,000 (approximately 60,000 new Turkish liras) or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to U.S. \$5,000 (approximately 6,000 new Turkish liras) or its equivalent in foreign currency notes out of the country. Turkey does have cross-border currency reporting requirements. Article 16 of the recently enacted MASAK law (see below) gives customs officials the authority to sequester valuables of travelers who make false or misleading declarations and imposes fines for such declarations.

MASAK was established by the 1996 anti-money laundering law as part of the Ministry of Finance. MASAK became operational in 1997, and it serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. MASAK has three functions: regulatory, financial intelligence, and investigative. MASAK plays a pivotal role between the financial and law enforcement communities.

In October 2006, Parliament enacted a new law reorganizing MASAK along functional lines, explicitly criminalizing the financing of terrorism, and providing safe harbor protection to the filers of STRs. The law also expands the range of entities subject to reporting requirements, to include several Designated Non-Financial Businesses and Professions (DNFBPs), such as art dealers, insurance companies, lotteries, vehicle sales outlets, antique dealers, pension funds, exchange houses, jewelry stores, notaries, sports clubs, and real estate companies. While the legislation has been improved to require reporting from a wide range of industries and entities, almost all STRs continue to be submitted by banks, which suggests inadequate supervision or regulation of these DNFBPs. It also specifies sanctions for failure to comply. The law gives MASAK the authority to instruct a number of different inspection bodies (such as the bank examiners, the financial inspectors or the tax inspectors) to initiate an investigation if MASAK has reason to suspect financial crimes. Likewise, MASAK can refer suspicious cases to the Public Prosecutor and the Public Prosecutor can ask MASAK to conduct a preliminary investigation prior to referring a case to the police for criminal investigation. In August 2007, a regulation on money laundering crime was enacted enforcing MASAK's authority to combat these crimes. However there continues to be limited training and specialization in, or understanding of, money-laundering and terrorist financing among law enforcement units and judicial authorities, resulting in a high number of acquittals in anti-money laundering and counter-terrorist financing (AML/CTF) cases.

According to MASAK statistics, as of December 31, 2006 it had pursued 2,231 money laundering investigations since its 1996 inception, but fewer than ten cases resulted in convictions. Moreover, all of the convictions are reportedly under appeal. Most of the cases involve nonnarcotics criminal actions or tax evasion; as of December 31, 2005, 41 percent of the cases referred to prosecutors were narcotics-related.

The GOT enforces existing drug-related asset seizures and forfeiture laws. MASAK, prosecutors, Turkish National Police, and the courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the anti-money laundering law, the Court of Peace—a minor arbitration court for petty offenses—has the authority to issue an order to freeze funds held in banks and nonbank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public Prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutors' Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours to decide whether to approve the action. There is no time limit on freezes. There is no specific provision in Turkish law for the sharing of seized assets with other countries; however the United States and Turkey have shared seized assets in one narcotics case.

MASAK's General Communiqué No. 3, dated February 2002, requires that a special type of STR be filed by financial institutions in cases of suspected terrorist financing. However, until the amendments to the criminal code were enacted in June 2006, terrorist financing was not explicitly defined as a criminal offense under Turkish law. Various existing laws with provisions that can be used to punish the financing of terrorism include articles 220, 314 and 315 of the Turkish penal code, which prohibit assistance in any form to a criminal organization or to any organization that acts to influence public services, media, proceedings of bids, concessions, and licenses, or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. The names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated list, as well as U.S.-designated names, are routinely distributed to financial institutions and appropriate Turkish agencies. However Turkey has failed to take steps to employ an effective regime to combat terrorist financing, especially as it relates to UNSCRs 1267 and 1373. For example, while the GOT has implemented UNSCR 1267, it has failed to establish punishment or sanctions for institutions that fail to observe a freezing order, and it has not established procedures for delisting entities or unfreezing funds. Additionally, the GOT has not taken steps that would allow it to freeze the assets of entities designated by other jurisdictions, as required under UNSCR 1373.

Another area of vulnerability in the area of terrorist financing is the GOT's supervision of nonprofit organizations. The nonprofit sector is well regulated, but it is not audited on a regular basis for CTF vulnerabilities and does not receive adequate AML/CTF outreach and guidance from the GOT. The General Director of Foundations (GDF) issues licenses for charitable foundations and oversees them. However, there are a limited number of auditors to cover more than 70,000 institutions. The Ministry of Interior regulates charitable nongovernmental associations (NGOs). The GDF, as part of the Ministry of Interior, keeps central registries of the charitable organizations they regulate and they require charities to verify and prove their funding sources and to have bylaws. Charitable organizations are required to submit periodic financial reports to the regulators. The regulators and the police closely monitor monies received from outside Turkey. The police also monitor NGOs for links to terrorist groups.

Alternative remittance systems are illegal in Turkey, and in theory only banks and authorized money transfer companies are permitted to transfer funds. Trade-based money laundering, fraud, and underground value transfer systems are also used to avoid taxes and government scrutiny. There are 21 free trade zones operating in Turkey. The GOT closely controls access to the free trade zones. Turkey is not an offshore financial center.

According to MASAK statistics, no assets linked to terrorist organizations or terrorist activities were frozen in 2006. Turkey has a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although the law allows only for their criminal forfeiture and not their administrative forfeiture. Article 7 of the anti-money laundering law provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (recently expanded to include crimes punishable by one year imprisonment), once the defendant is convicted. The law allows for the confiscation of the equivalent value of direct proceeds that could not be seized. Instrumentalities of money laundering can be confiscated under the law. In addition to the anti-money laundering law, Articles 54 and 55 of the Criminal Code provide for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money or support terrorist activity, or are related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

In the months after 9/11, the Council of Ministers decreed (2482/2001) all funds and financial assets of individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list be frozen. However, the tools available at that time under Turkish law for locating, freezing, seizing, and confiscating terrorist assets were cumbersome, limited, and ineffective. In late 2001, the Council of Ministers froze the funds of one individual accused of financing terror in Turkey. This individual filed an appeal in 2001, and in June 2006 the 10th Chamber of the Turkish Administrative Court overruled the original Council of Ministers decision on technical grounds. The 10th Chamber's decision was appealed, and upon review, in February 2007 the Highest Chamber Council of the Turkish Administrative Court upheld the original decision to freeze the individual's assets on the grounds that there were no legal irregularities in the original decision. The assets of the 1267-listed individual continue to be frozen. Since then, changes in the law relating to MASAK, the Turkish criminal code, and the anti-terrorism law give more authority to seize and freeze assets quickly and make the Turkish system more compliant with international standards.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. Turkey is a member of the Financial Action Task Force (FATF). Since 1998, MASAK has been a member of the Egmont Group of Financial Intelligence Units. Turkey is a party to the 1988 UN Drug Convention, the UN International Convention for Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. In January 2005, Turkey became a party to the Council of Europe (COE) Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime.

With the passage of several new pieces of legislation, the Government of Turkey took steps in 2006 and 2007 to strengthen its AML/CTF regime. The GOT now faces the challenge of aggressively implementing these laws. In 2007 the GOT established a High Coordination Council on Financial Crimes, which consists of MASAK, Finance Ministry, Capital Markets Board, and Central Bank representatives. The aim of this board is to improve coordination among the agencies to combat financial crimes and support the work of MASAK. MASAK must improve its automation to be able to access banks' and other financial institutions' data bases, so as to accelerate MASAK's process and enable it to refer cases more quickly to prosecutors. The lack of prosecutions and convictions for money laundering is troubling. Law enforcement and judicial authorities need to be given additional training and develop expertise on AML/CTF issues. There is an over-reliance on STRs to initiate money laundering investigations in Turkey. Law enforcement and customs authorities should be enabled to follow the money and value trails during the course of their investigations, and should not be required to turn that portion of the investigation over to MASAK. MASAK should second members of the Turkish National Police and prosecution offices in order fulfill its mandate to investigate

preliminary indications of money laundering. As currently staffed, MASAK does not have criminal investigative experience although it is required to make such initial determinations. The GOT should also regulate and investigate remittance networks to thwart their potential misuse by terrorist organizations or their supporters. The GOT needs to fully implement the provisions of UNSCRs 1267 and 1373, and should consider expanding its narrow legal definition of terrorism, which currently is limited to acts committed by members of organizations against the Turkish Republic by pressure force and violence using terror, intimidation, oppression or threat. The GOT should also strengthen its oversight of foundations and charities, which currently receive only cursory overview and auditing. Turkey should take steps to improve the CDD procedures and other preventative measures, as well as adopt a risk-based approach to AML/CTF. Supervision and regulation of DNFBPs covered by the 2006 legislation also needs to be improved.

Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). The TCI is comprised of two island groups and forms the southeastern end of the Bahamas archipelago. The U.S. dollar is the currency in use. The TCI has a significant offshore center, particularly with regard to insurance and international business companies (IBCs). Its location has made it a transshipment point for narcotics traffickers. The TCI is vulnerable to money laundering because of its large offshore financial services sector, as well as its bank and corporate secrecy laws and Internet gaming activities. As of 2006, the TCI's offshore sector has eight banks, four of which also offer offshore banking; approximately 2,500 insurance companies; 20 trusts; and 17,000 "exempt companies" that are IBCs. No updated statistics are available for 2007.

The Financial Services Commission (FSC) licenses and supervises banks, trusts, insurance companies, and company managers. It also licenses IBCs and acts as the Company Registry for the TCI. These institutions are subject to on-site examination to determine compliance with TCI laws and regulations. The Financial Services Commission has a staff of 21, including four regulators. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in 2002. It reports directly to the Governor, as well as to the Minister of Finance. The FSC is in the process of adopting a risk-based examination approach to better assess, identify, measure, monitor and control threats associated with potential money laundering and terrorist financing.

The offshore sector offers "shelf company" IBCs, and all IBCs are permitted to issue bearer shares. However, the Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined licensed custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts insulating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative powers and may assist overseas regulators. Currently, the FSC is rewriting the trust legislation with assistance from the UK Government.

The 1998 Proceeds of Crime Ordinance (PCO) criminalizes money laundering related to all crimes and provides "safe harbor" protection for good faith compliance with reporting requirements. The PCO allows for the criminal forfeiture of assets related to money laundering and other offenses, although civil forfeiture is not permitted. The PCO also establishes a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze and disseminate financial disclosures such as suspicious activity reports (SARs). Its members also include the following individuals or their designees: Collector of Customs, the Managing Director of the FSC and the Head of its Financial Crimes Unit (FCU), the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

The Proceeds of Crime (Money Laundering) Regulations came into force in 2000. The Money Laundering Regulations place additional requirements on the financial sector such as identification of customers, retention of records for a minimum of ten years, training staff on money laundering prevention and detection, and development of internal procedures to ensure proper reporting of suspicious transactions. The Money Laundering Regulations apply to banks, insurance companies, trusts, mutual funds, money remitters, investment dealers, and issuers of credit cards. However, there is no supervisory or regulatory authority to oversee regulatory compliance by money remitters and investment dealers. Other sectors, such as gambling, jewelers, real estate companies, and currency exchange companies, are not subject to the Money Laundering Regulations. Although the customer identification requirements only apply to accounts opened after the Regulations came into force, TCI officials have indicated that banks are required to conduct due diligence on previously existing accounts.

As with the other United Kingdom Caribbean overseas territories, the Turks and Caicos underwent an evaluation of its financial regulations in 2000, cosponsored by the local and British governments. The report noted several deficiencies and the government has moved to address most of them. The report noted the need for improved supervision, which the government acknowledged. An Amendment to the Banking Ordinance was introduced in February 2002 to remedy deficiencies outlined in the report relating to notification of the changes of beneficial owners, and increased access of bank records to the FSC. However, legislation has not been introduced to remedy the deficiencies noted in the report with respect to the Superintendent's lack of access to the client files of Company Service and Trust providers, nor is there legislation that clarifies how the Internet gaming sector is to be supervised with respect to anti-money laundering compliance.

In 1999, the FSC, acting as the secretary for the MLRA, issued nonstatutory Guidance Notes to the financial sector, to help educate the industry regarding money laundering and the TCI's anti-money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all SARs to the Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police Force, which analyzes and investigates financial disclosures. The FCU also acts as the TCI's financial intelligence unit (FIU). No statistics are available on the number of SARs received by the FCU in 2007, nor are there current statistics on the number of investigations, prosecutions, or convictions.

Travelers entering or leaving the TCI with more than U.S. \$10,000 must make a declaration to Customs officials. In November 2007, a Bahaman citizen who entered TCI with over U.S. \$14,000 in cash was arrested for making a false declaration after completing a Customs form stating that he was traveling with less than \$10,000. The investigation of this incident marks the first time Customs and the FCU have worked together on a joint investigation. In 2007, the FCU also assisted Canadian law enforcement in the investigation of two Canadian citizens, who were charged with fraud and money laundering in September.

As a UK territory, the TCI is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. However, the Government of the TCI has not yet implemented domestic orders that would criminalize the financing of terrorism. The UK's ratification of the International Convention for the Suppression of the Financing of Terrorism has not been extended to the TCI.

The TCI cooperates with foreign governments—in particular, the United States and Canada—on law enforcement issues, including narcotics trafficking and money laundering. The FCU also shares information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign

regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents.

The TCI is subject to the 1988 UN Drug Convention. The TCI is a member of the Caribbean Financial Action Task Force, and underwent a mutual evaluation in September 2007. The results of the mutual evaluation should be presented to the CFATF plenary in 2008. TCI's FIU is not a member of the Egmont Group of financial intelligence units. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990. The TCI does not have a Tax Information Exchange Agreement with the United States.

The Government of the Turks and Caicos Islands has put in place the relevant legislative framework to combat money laundering, but needs to implement relevant provisions of its anti-money laundering regime, criminalize terrorist financing, ensure that its FIU is fully functioning, and ensure that money laundering cases are investigated and prosecuted. The Government of the TCI should reform its current regulatory structure to be in full accordance with international standards by extending existing regulations to all sectors, bringing all obligated entities under the supervision of a regulatory body, and enhancing its on-site supervision program. The Turks and Caicos Islands should take the necessary steps to ensure that its FIU is eligible for membership in the Egmont Group of financial intelligence units. The Government of the TCI should criminalize the financing of terrorists and terrorism. The TCI should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands should also provide adequate resources and authorities to provide supervisory oversight of its offshore sector to further ensure criminal or terrorist organizations do not abuse the Turks and Caicos Islands' financial sector.

Ukraine

Corruption, organized crime, prostitution, smuggling, tax evasion, trafficking in persons, drugs and arms, and other organized criminal activity continue to be sources of laundered funds in Ukraine. As of October 1, 2007, Ukraine had approximately 173 active banks, two of which are state-owned. There are no offshore financial centers or facilities under Ukraine's jurisdiction.

Ukraine's 2005 budget eliminated the tax and customs duty privileges available in eleven Special Economic Zones (SEZs) and nine Priority Development Territories (PDTs) that had been associated with rampant evasion of customs duties and taxes. In late 2006, a government no longer in power registered a draft law with Parliament to restore tax and customs privileges for businesses operating in the SEZs. The law never came to a final vote, and the new government that assumed power in late 2007 has said that it will not reintroduce the privileges.

In January 2001, the Government of Ukraine (GOU) enacted the "Act on Banks and Banking Activities," which introduced some anti-money laundering (AML) requirements for banking institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. In August 2001, the President signed the "Law on Financial Services and State Regulation of the Market of Financial Services." This law establishes regulatory control over nonbank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." The law provides definitions for "financial institutions" and "services," imposes record-keeping requirements on obligated entities, and identifies the responsibilities of regulatory agencies. The law established the State Commission on Regulation of Financial Services Markets, which, along with the National Bank of Ukraine (NBU) and the State Commission on Securities and the Stock Exchange, has responsibility for regulating financial services markets.

The Financial Action Task Force (FATF) placed Ukraine on the list of noncooperative countries and territories (NCCT) in September 2001. After a number of unsuccessful legislative attempts to develop an anti-money laundering (AML) regime that met international standards, the FATF called upon its members to invoke countermeasures in December 2002. At that time, the U.S. designated Ukraine as a jurisdiction of primary money laundering concern, under Section 311 of the USA PATRIOT Act. The GOU passed comprehensive AML legislation in February 2003, and promised significant institutional reform. The FATF withdrew its call for members to invoke countermeasures, after which the United States revoked its USA PATRIOT Act designation of the GOU as a jurisdiction of primary money laundering concern. The FATF removed Ukraine from the NCCT list in February 25, 2004.

Ukraine's legislation requires banks and other financial service providers to implement AML compliance programs: conduct due diligence to identify beneficial owners prior to allowing the opening of an account or conducting certain transactions; report suspicious transactions to the national financial intelligence unit (known as the State Committee for Financial Monitoring, or "SCFM") and maintain records on suspicious transactions; and, for a period of five years. The legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. In August 2003, the State Commission established the State Register of financial institutions, and by March 2007, the State Register contained information on 1,956 nonbank financial institutions.

Since November 2004, the GOU has made several efforts to pass a set of amendments to the AML law to bring Ukraine's regime into compliance with FATF's revised Forty plus Nine recommendations. The Verkhovna Rada, Ukraine's Parliament, twice rejected the government's draft in 2005. The government redrafted the law, narrowing its scope to the FATF recommendations and omitting provisions introducing a new SCFM authority and other bureaucratic changes that had drawn opposition in the Parliament. Among other provisions, the new legislation would expand the sectors subject to primary monitoring to include retail traders, lawyers, accountants, and traders of precious metals. The draft law, entitled "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing," was passed by the Parliament on June 19, 2007 but not signed into law. Because the draft law passed during a period when the authority of the Parliament was not recognized by the President, the draft law will now again need to be addressed by the Parliament.

In 2004, authorities reduced the threshold for compulsory financial monitoring from Ukrainian Hryvnias (UAH) 300,000 (approximately U.S. \$59,430) for cashless payments and UAH 100,000 (approximately U.S. \$19,800) for cash payments, to UAH 80,000 (approximately U.S. \$15,848) for payments using either method. The compulsory reporting threshold exists only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction suspected of being connected to terrorist activity must be reported to the appropriate authorities immediately.

Cash smuggling is substantial in Ukraine, although it is reportedly related more closely to unauthorized capital flight rather than to criminal proceeds or terrorist funding. In 2005, the GOU sought to combat smuggling and corruption by reducing import duties, introducing new procedures for the Customs Service, and implementing transparent procedures for the privatization of state enterprises. As of August 2005 travelers are required to declare cross-border transportation of cash sums in excess of U.S. \$3,000, and declare the origin of funds exceeding U.S. \$10,000.

In January 2006, Ukraine enacted Law 3163-IV, which amended the initial AML laws. Under this law, the entities obligated to conduct initial financial monitoring must be able to provide proof that they are fulfilling all Know Your Customer (KYC) identification requirements. Ukraine also granted state agencies enhanced authority to exchange information internationally, improved rules on bank organization, and implemented a screening requirement at the level of financial institutions. On September 14, 2006, Ukraine enacted amendments to the "Law on Banks and Banking" that require all

banks to be formed as open joint-stock companies or as cooperatives. This measure strengthens disclosure requirements on the identity of the beneficial owners of banks. These amendments apply to all newly formed banks and provide a three-year period for existing banks to comply. As a result of these and other improvements to its legal framework, the FATF in February 2006 suspended its direct monitoring of Ukraine.

The Criminal Code of Ukraine has separate provisions criminalizing drug-related and nondrug-related money laundering. Amendments to the Code adopted in January 2003 included willful-blindness provisions and expanded the scope of predicate crimes for money laundering to include any action punishable under the Criminal Code with at least three years of imprisonment, excluding certain specified actions.

The SCFM is Ukraine's financial intelligence unit (FIU). The December 10, 2001 Presidential Decree "Concerning the Establishment of a Financial Monitoring Department" mandated the establishment of the SCFM as Ukraine's FIU. The SCFM became operational on June 12, 2003 and is the sole agency authorized to receive and analyze financial information from financial institutions. On March 18, 2004, Ukraine's Rada granted the SCFM the status of a central executive agency, subordinate to the Cabinet of Ministers. However, a draft law "On the Opposition," which was submitted to the Parliament in early 2007, specifies that the Parliament's opposition party could assign persons to certain leadership jobs in a number of state agencies, including the SCFM. Specifically, the draft law reserves the job of director and of two of the four deputy director positions to the opposition party in the Parliament. The law, if enacted, would likely contradict the November 2002, Law on Money Laundering Prevention. By year-end, the Parliament had taken no action on this draft.

The SCFM is an administrative agency with no investigative or arrest authority. It is authorized to collect suspicious transaction reports and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. As of October 1, 2007, the SCFM had established 22 local branches. The SCFM is authorized to conclude interagency agreements and exchange intelligence on financial transactions involving money laundering or terrorist financing with other FIUs. As of October 2007, the SCFM had concluded memoranda of understanding (MOUs) with thirty-three foreign FIUs, including FinCEN. It has become a regional leader with regard to the volume of case information exchanged with counterpart FIUs.

The SCFM collects and analyzes data, and identifies possible cases for prosecution to the Prosecutor General's Office (PGO). Although the SCFM is an administrative unit, it has processed, analyzed and developed some cases to the point of establishing probable cause before referring a case for further investigation. In 2006, the SCFM received 841,589 transaction reports, which include both STRs and automatic threshold reports. Banks filed the majority of the reports. The SCFM sent 446 separate cases to law enforcement agencies and the Prosecutor General's Office (PGO) for "active research". As a result of subsequent investigation of these cases, law enforcement agencies initiated 164 criminal cases in 2006. Of these, prosecutors brought only eight cases to trial, with only one conviction. In the period 2003 through 2006, twenty of 325 cases went to trial with, with only three resulting in convictions on charges of money laundering.

Although the reporting system is effective and the SCFM has generated a substantial number of probable cases for referral, it has not led to a meaningful number of convictions. Many observers believe that the low prosecution rate is caused by a reluctance of the PGO to pursue the cases referred by the SCFM. Local prosecutors may close money laundering investigations and cases prematurely or arbitrarily, possibly because of lack of sufficient manpower or resources or because of corruption. Other possible reasons include a weak understanding of money laundering crimes (prosecutors often identify tax evasion with money laundering, for example) and a belief that other types of crimes should take priority over money laundering.

The SCFM acknowledges the existence and use of alternative remittance systems in Ukraine. In 2007, the Security Service of Ukraine published a report signaling that hawala might be on the rise in Ukraine due to a large number of Ukrainians working abroad and the growth of foreign communities in Ukraine. The SCFM and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

Ukraine has an asset forfeiture regime. Article 59 of the Ukrainian Criminal Code provides for the forceful seizure of all or a part of the property of a person convicted for grave and particularly grave offenses as set forth in the relevant part of the code. With respect to money laundering, Article 209 allows for the forfeiture of criminally obtained money and other property.

On December 10, 2003, the Cabinet of Ministers issued Decree No. 1896, establishing a Unified State Information System of Prevention and Counteraction of Money Laundering and Terrorism Financing. The system, which became fully operational in December 2006, provides the SCFM with unobstructed access to the databases of twelve ministries and agencies, including the Ministries of Internal Affairs, Economy and Finance, as well as the State Tax Administration, State Security Service, State Customs Administration, State Property Fund, State Statistics Administration, Border Guard Service, Securities Commission, Financial Services Commission, and Control and Revision Department.

On September 21, 2006, the Rada enacted revisions to Article 258 of the Criminal Code, adding Article 258-4 that explicitly criminalizes terrorist financing. The revised text mandates imprisonment from three to eight years for financing, material provision, or provision of arms with the aim of supporting terrorism. The revisions also amend the criminal procedure code to empower the State Security Service (SBU) with primary responsibility for investigation of terrorist financing.

Law 3163-IV enhanced Ukraine's ability to exchange information internationally and placed greater obligations on banks to combat terrorist financing. This Law requires banks to adopt procedures to screen parties to all transactions using an SCFM-issued list of beneficiaries of, or parties to, terrorist financing. Banks must freeze assets for two days and immediately inform the SCFM and law enforcement bodies whenever a party to a transaction appears on the list. The SCFM can extend the freeze to five days. On October 25, 2006, the Cabinet of Ministers approved the SCFM's list, drawn from three sources: the United Nations 1267 Sanctions Committee's consolidated list; information from the Ukrainian Security Service on individuals and entities suspected of violating article 258 of the Ukrainian Criminal Code concerning terrorism; and the lists compiled by those countries that have bilateral agreements with Ukraine on mutual recognition of terrorist designations.

The GOU has cooperated with U.S. efforts to track and freeze the financial assets of terrorists and terrorist organizations. Banks and nonbank financial services also receive these U.S. designations, and are instructed to report any transactions involving designated individuals or entities.

The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. Additionally, the two countries have a bilateral taxation agreement that provides for the exchange of information in administrative, civil, and criminal matters related to taxation and tax evasion.

Ukraine is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Ukraine has signed, but has yet to ratify, the UN Convention against Corruption (UNCAC). Ukraine is a member of MONEYVAL, a FATF-style regional body (FSRB). The SCFM is a member of the Egmont Group.

Ukraine has strengthened and clarified its newly adopted laws. With the SCFM, the NBU, and other entities in the financial and legal sectors, Ukraine has established a comprehensive AML regime. To date, however, Ukraine's ability to implement this regime through consistent successful criminal prosecutions remains unproven. Both law enforcement officers and the judiciary need a better

understanding of the theoretical and practical aspects of investigating and prosecuting money laundering cases. Law enforcement agencies should give higher priority to investigating money laundering cases. The Prosecutor General's Office should address the deficiencies of that office, particularly in its organization and staff training. The GOU should establish oversight capabilities of local investigators, prosecutors, and judges to insure that cases are vigorously pursued and prosecuted. Ukraine's authorities should take steps to better understand the depth of their country's alternative remittance systems, and begin to address a monitoring and reporting regime. Likewise, Ukraine should take steps to enact a regulatory regime for charitable and nonprofit organizations that goes beyond monitoring. Ukraine should ratify the UNCAC and more aggressively address its public corruption problem by prosecuting and convicting corrupt public officials.

United Arab Emirates

The United Arab Emirates (UAE) is an important financial center in the Gulf region. Although the financial sector is modern and progressive, the UAE remains a largely cash-based society. Dubai, in particular, is a major international banking center. The country also has a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people, goods, and capital. The UAE is particularly susceptible to money laundering due to its geographic location as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia; its expanding trade ties with the countries of the former Soviet Union; and lack of transparency in its corporate environment.

The potential for money laundering is exacerbated by the large number of resident expatriates (roughly 80 percent of total population) who send remittances to their homelands. Given the country's proximity to Afghanistan, where most of the world's opium is produced, narcotics traffickers are increasingly reported to be attracted to the UAE's financial and trade centers. Other money laundering vulnerabilities in the UAE include hawala, trade fraud, smuggling, the real estate boom, the misuse of the international gold trade, and conflict diamonds.

The Central Bank is responsible for supervising the UAE's financial sectors, which include banks, exchange houses, and investment companies. It is authorized to issue licenses and impose administrative sanctions for compliance violations. The Central Bank also has the authority to issue instructions and recommendations to financial institutions as it deems appropriate, and to take any measures as necessary to ensure the integrity of the UAE's financial system. Following the September 11, 2001 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities. In close concert with the United States, the UAE imposed a freeze on the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both national and emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's reputation and security. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing.

The UAE has enacted the Anti-Money Laundering Law No. 4/2002, and the Anti-Terrorism Law No. 1/2004. Both pieces of legislation, in addition to the Cyber Crimes Law No. 2/2006, serve as the foundation for the country's anti-money laundering and counter-terrorist financing (AML/CTF) efforts. Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding 2000 dirhams (approximately \$545) and currency imports above 40,000 dirhams (approximately U.S. \$10,900). The law imposes criminal penalties for money laundering that includes up to seven years in prison plus a fine of up to 300,000 dirhams (approximately U.S. \$81,700), as well as a seizure of assets upon conviction. The law also provides safe harbor provisions for reporting officers.

Prior to the passage of the Anti-Money Laundering Law, the National Anti-Money Laundering Committee (NAMLC) was established in July 2000 to coordinate the UAE's anti-money laundering policy. The NAMLC was later codified as a legal entity by Law No. 4/2002, and is chaired by the Governor of the Central Bank. Members of the NAMLC include representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, Secretary General of the Municipalities, Federation of the Chambers of Commerce, and five major banks and money exchange houses (as observers).

Administrative Regulation No. 24/2000 provides guidelines to financial institutions for monitoring money laundering activity. This regulation requires banks, money exchange houses, finance companies, and any other financial institutions operating in the UAE to follow strict "know your customer" guidelines. Financial institutions must verify the customer's identity and maintain transaction details (i.e., name and address of originator and beneficiary) for all exchange house transactions over the equivalent of U.S. \$545 and for all nonaccount holder bank transactions over U.S. \$10,900. The regulation delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Regulation 24/2000 call for customer records to be maintained for a minimum of five years and further require that they be periodically updated as long as the account is open.

In July 2004, the UAE government strengthened its legal authority to combat terrorism and terrorist financing by passing Federal Law Number No. 1/2004. The Law specifically criminalizes the funding of terrorist activities and terrorist organizations. It sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "nonconventional weapons" and their components that are intended for use in a terrorist activity.

Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," regardless whether the terrorist acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits, transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity as defined in the law.

The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint. Law No. 1/2004 also established the "National Anti-Terror Committee" (NATC) to serve as the government's interagency liaison with respect to implementing the United Nations Security Council Resolutions (UNSCR) on terrorism, and sharing information with its foreign counterparts as well as with the United Nations. Representatives from Ministries of Foreign Affairs, Interior, Justice, and Defense; Central Bank; State Security Department; and Federal Customs Authority comprise the NATC.

The Central Bank also ensures that it circulates an updated UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations to all the financial institutions under its supervision. In 2007, the UAE took steps toward fulfillment of its UN nonproliferation obligations. On August 31, 2007 the UAE issued Law No. 13 of 2007 on export and import controls. With regard to the UAE's UNSCR 1737 and 1747 commitments, the UAE Central bank ordered banks and other financial institutions to freeze accounts or deposits of designated entities. It also ordered financial

institutions to cease transfers on behalf of designated entities and to refrain from entering into new commitments for grants, financial assistance, and concession loans to the Iranian Government

The Anti-Money Laundering and Suspicious Case Unit (AMLSCU) was established in 2002 as the UAE's financial intelligence unit (FIU), and was housed within the Central Bank. In addition to receiving Suspicious Transaction Reports (STRs), the AMLSCU is authorized to send information requests to foreign regulatory authorities to conduct its preliminary investigations based on suspicious transaction report data. The AMLSCU joined the Egmont Group in June 2002. As of October 2007, the AMLSCU has received and investigated a total of 4392 suspicious transactions reports (STRs), for the period of December 2000 until April 2007. The AMLSCU reports that it has issued a total of 42 freeze orders in response to STRs between December 2000 (prior to the establishment of the FIU) and October 2006.

It is unclear how many money laundering prosecutions have taken place in the UAE in 2007. However, there were two high profile money laundering cases in the UAE during the 2006/2007 timeframe. In November, the Sharjah Appeals Court upheld a verdict sentencing seven men to five years in prison for money laundering. An Abu Dhabi court also sentenced two of the individuals to life imprisonment for drug trafficking and the rest to ten year sentences for drug trafficking. The individuals were arrested in 2006 for attempting to smuggle 2.5 tons of hashish from Pakistan to Holland, via Sri Lanka, the UK, and Belgium. UAE authorities worked with law enforcement officials in the respective countries to track the shipment. In October 2007, the Dubai police referred 48 suspects to the Public Prosecutors on charges of money laundering and abetting drug trafficking.

Several amendments were made to the Central Bank Regulations 24/2000 in July 2006. First, the regulations added the term "terrorist financing" to any references made to the term "money laundering." Second, the regulations required financial institutions to freeze transactions that they believe may be destined for funding terrorism, terrorist organizations, or for terrorist purposes. The regulations also require financial institutions to notify the AMLSCU in writing of such transactions "in case of any doubt". Finally, enhanced due diligence requirements for charities were promulgated, requiring banks to obtain a certificate from the Minister of Social Affairs before opening or maintaining any charitable organization-type account.

In 2006, the UAE enacted Law No. 2/2006 of the Cyber Crimes. Article 19 of the law criminalized the electronic transfer of money or property through the Internet in which the true sources of such assets are either concealed or linked to criminal proceeds. Violations are punishable by up to seven years imprisonment and fines ranging from approximately \$8,170 to \$54,500. Article 21 of the law outlaws the use of the Internet to finance terrorist activities, promote terrorist ideology, disseminate information on explosives, or to facilitate contact with terrorist leaders. Any violation of Article 21 is punishable by up to 5 years imprisonment.

Hawala is where money laundering activity is likely more prevalent due to the largely undocumented nature of this informal remittance system. Dubai is a regional hawala center. Hawala is an attractive mechanism for terrorist and criminal exploitation due to its nontransparency to law enforcement and regulators and the highly resilient nature of the system. In 2002, the Central Bank issued new regulations to help improve the oversight of hawala. The new regulations required hawala brokers (hawaladars) to register with the Central Bank, submit the names and addresses of all originators and beneficiaries of funds, and to file suspicious transaction reports on a monthly or quarterly basis. However, since the inception of the program, there reportedly have not been any suspicious reports filed by hawaladars.

As of October 2007, the Central Bank had registered 246 hawaladars, with an additional 70 applicants working to complete their registration requirements. Once registered, the Central Bank conducts one-on-one training sessions with each registered hawaladar to ensure that dealers understand the record-keeping and reporting obligations. The registered hawaladars are also required to use an account they

open at the Central Bank to process their transactions. Currently, there is no accurate estimate of the total number of UAE-based hawala brokers, and there is no penalty for failure of hawaladars to register with the Central Bank. Officials argue that the registration program is still in the initial phase of determining the magnitude of the industry. As of August 2007, the Central Bank reported that it had received over 800 quarterly activity reports from hawaladars.

The UAE has not set any limits on the amount of cash that can be imported into or exported from the country. No reporting requirements exist for cash exports. However, the Central Bank requires that any cash imports over \$10,900 must be declared to Customs; otherwise undeclared cash may be seized upon attempted entry into the country. All cash forfeiture cases are handled at the judicial level because there are no administrative procedures to handle forfeited cash. Still, enforcement mechanisms are lax. Customs officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities, arguing that the UAE is a cash-based economy, and it is not unusual for people to carry significant sums of cash.

Dubai remains the center of the UAE's burgeoning diamond trade, although new facilities are springing up in the Emirate of Ras Al Khaimah as interest spreads in the lucrative business. The UAE has been a participant in the Kimberley Process Certification Scheme for Rough Diamonds since November 2002, and began certifying rough diamonds exported from the UAE on January 1, 2003. Law No. 13 of 2004 regulates supervision of Import/Export and Transit of Rough Diamonds. Article 5 of the law prohibits the import of rough diamonds, unless they are accompanied by a Kimberley Process certificate and in a sealed, tamper resistant container.

The Dubai Diamond Exchange (DDE), a subsidiary of the Dubai Multi Commodities Center (DMCC), is a quasi-governmental organization charged with issuing Kimberley Process (KP) certificates in the UAE. Prior to January 1, 2003, the DMCC circulated a sample UAE certificate to all KP participant states and embarked on a public relations campaign to familiarize the then estimated 50 diamond traders operating in Dubai with the new KP requirements. There are more than 300 firms involved in diamond trading in Dubai. Under the KP regulations, UAE Customs is the sole point of entry for both rough and finished diamonds to the UAE. Customs officials are authorized to delay or even confiscate those diamonds entering the UAE that do not have the proper certificates.

In 2006, Russian customs officials reportedly apprehended an air passenger from Dubai after he tried to smuggle 2.5 kilos of diamonds into the country. There are also reports that diamonds are increasingly being used as a medium to provide counter valuation in hawala transfers, particularly between Dubai and Mumbai.

The former head of the Dubai Diamond Exchange implemented enhanced monitoring measures in compliance with the Moscow Resolution on Cote d'Ivoire of November 2005, but two suspect diamond shipments of questionable provenance released by the DDE in 2006 and 2007 indicate continuing weaknesses in the process. The UN Group of Experts on Cote d'Ivoire, visiting Dubai in May 2007, raised with the DDE the release in September 2006 and January 2007, respectively, of two shipments of diamonds with suspect Ghanaian certificates of origin. In both cases the World Diamond Council was requested to verify the origin of the diamonds. In the first instance the Working Group of Diamond Experts concluded that the assessed diamonds bore characteristics unknown in Ghanaian diamonds, but possibly consistent with stones from Guyana or Brazil. In the second case, the diamonds were released before the WDC's final report was released. The UN Group of Experts on Cote d'Ivoire also reported that individuals in Dubai's Gold Land stated that they had in their possession large quantities of African diamonds without Kimberley Process certification.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, the SCA issued anti-money laundering guidelines to all brokers that included identity verification instructions for new customer accounts, a reporting requirement for cash transactions above U.S. \$10,900, and a minimum five-year record keeping requirement for all customer account

information. The SCA also instructed brokers to file suspicious transaction reports with the SCA for initial analysis before they are forwarded to the AMLSCU for further action.

The UAE's real estate market continues to grow with the various emirates following Dubai's model of opening up some property ownership to expatriates. Dubai's real estate market grew significantly in 2007, making this sector another area that is susceptible to money laundering abuse. In 2002, Dubai began to allow three real estate companies to sell "freehold" properties to noncitizens. Since then, several other emirates have followed suit. For instance, Abu Dhabi has passed a property law, which provides for a type of lease-hold ownership for noncitizens. In addition, citizens of GCC countries have the right to purchase and trade land within designated investment areas, while other expatriates are permitted to invest in real estate properties for a 99-year leasehold basis. Due to the intense interest in and reported cash purchases of such properties, the potential for money laundering has become of increased concern to the UAE Government. As a result, developers have stopped accepting cash purchases for these properties. The UAE does not have a central database to show registered property owners within the UAE, which encumbers international money laundering investigations.

Since the September 11, 2001 terrorist attacks, the UAE Government (UAEG) has been more sensitive to regulating charitable organizations and accounting for funds transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance.

Charities are regulated by the UAE Ministry of Social Affairs, which is responsible for licensing and monitoring registered charities in these emirates. The Ministry also requires these charities to keep records of all donations and beneficiaries, and to submit financial reports annually. Charities in Dubai are licensed and monitored by the Dubai Department of Islamic Affairs and Charitable Activities. Some charities, however, particularly those located in the Northern Emirates, are only registered with their local emirate authority and not the federal Ministry. In July 2006, Regulation 24/2000 was amended, requiring charities from all emirates to obtain a certificate from the Minister of Social Affairs before being permitted to open or maintain bank accounts in the UAE. This amendment effectively required that all charities must be registered federally and no longer at just the emirate level. In November 2006, the UAE hosted a United Kingdom/Gulf Cooperation Council conference on charities, and made a proposal to hold biannual meetings going forward with the UK and GCC on charities oversight.

The UAE has both free trade zones (FTZs) and one financial free zone (FFZ). The number of FTZs is growing, with 37 operating in the UAE. Every emirate except Abu Dhabi has at least one functioning FTZ. The free trade zones are monitored by the local emirate rather than federal authorities.

There are over 5,000 multinational companies located in the FTZs, and thousands more individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are considered offshore or foreign entities for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit nonresidents to open bank accounts in the UAE. The larger FTZs in Dubai (such as Jebel Ali free zone) are well-regulated. Although some trade-based money laundering undoubtedly occurs in the large FTZs, a higher potential for financial crime exists in some of the smaller FTZs located in the northern emirates.

In March 2004, the UAEG passed Federal Law No. 8, regarding the Financial Free Zones (FFZs) (Law No. 8/2004). Although the new law exempts FFZs and their activities from UAE civil, and commercial laws, FFZs and their operations are still subject to federal criminal laws including the

Anti-Money Laundering Law (Law No. 4/2002) and the Anti-Terror Law (Law No. 1/2004). As a result of Law 8/2004 and a subsequent federal decree, the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC), was established in September 2004. By September 2005, the DIFC had opened its securities market, the Dubai International Financial Exchange (DIFX).

Law No. 8/2004 limits the issuance of licenses for banking activities in the FFZs to branches of companies, joint companies, and wholly owned subsidiaries provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the FFZ from dealing in UAE currency (i.e., dirham), or taking "deposits from the state's markets." Further, the law stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The law empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the financial free zone, as well as the licensing of any UAE stock broker. Insurance activities conducted in the FFZ are limited by law to reinsurance contracts only. The law further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet.

In 2007 the Cabinet issued Resolution No. 28 that provided implementing regulations for financial free zones. The regulations specify that FFZs submit their semi-annual reports on activities and compliance to the UAE Cabinet. The regulations also spell out that inspections of FFZs will be carried out by cabinet resolution through a ministerial committee. These inspections will be carried out in cooperation with the FFZs. Results will be referred to the cabinet for action. The Regulation also instructs the FFZs to enter into Memorandums of Understanding (MOUs) with relevant authorities, such as the Central Bank, the Ministry of Economy, the Securities and Commodities Authority, and the Insurance Authority, for the purposes of better coordination, cooperation, and control.

DIFC regulations provide for an independent regulatory body, namely the Dubai Financial Services Authority (DFSA), to report its findings directly to the office of the Dubai ruler and an independent Commercial Court. According to DFSA regulators, the DFSA due diligence process is a risk-based assessment that examines a firm's competence, financial soundness, and integrity. Prior to the inauguration of the DIFC in 2004, several observers called into question the independence of the DFSA as a result of the high profile firings of the chief regulator and the head of the regulatory council (i.e., the supervisory authority). Subsequent to the firings, Dubai passed laws that gave the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, who modeled its regulatory regime after the United Kingdom, is the sole authority responsible for issuing licenses to those firms providing financial services in the DIFC.

The DFSA has licensed 156 institutions to operate within the DIFC as authorized firms licensed to carry on financial services in or from the DIFC. The DFSA also regulates ancillary service providers (provide legal or accountancy services in the DIFC). The DFSA prohibits offshore casinos or Internet gaming sites in the UAE, and requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). To date, there have been 18 suspicious transaction reports issued from firms operating in the DIFC (nine in 2007). Although firms operating in the DIFC are subject to Law No. 4/2002, the DFSA has issued its own anti-money laundering regulations and supervisory regime, which has caused some ambiguity about the Central Bank's and the AMLSCU's respective authorities within the DIFC. Ongoing discussions continue between the DFSA and the UAE Central Bank to create a formal bilateral arrangement.

As a result, the DIFC acknowledged the need to enhance its regulatory and compliance authority. On July 18, 2007, it enacted regulations for nonfinancial Anti-Money Laundering Anti Terrorist Finance which applies Financial Action Task Force (FATF) compliant requirements in the DIFC jurisdiction to real estate agents, dealers in precious metals and stones, dealers in high value goods (cash payments of

over U.S. \$15,000), non-Authorized Service Providers, lawyers, accountants, auditors, and non-DFSA regulated Trust and Company Service Providers. These regulations do not apply to DFSA regulated firms. With regard to auditors and accountants, for example, this would apply to those that do not audit authorized firms. The DFSA has undertaken a campaign to reach out to other international regulatory authorities to facilitate information sharing. As of November 2007, the DFSA has MOUs with several other regulatory bodies, including the UK's Financial Services Authority (FSA), the Emirates Securities and Commodities Authority, and the U.S. Commodity Futures Trading Commission (CFTC). On October 23, 2007, the DFSA entered into a MOU with the five U.S. banking supervisors.

The UAE is a party to the 1988 UN Drug Convention and to all twelve UN conventions and protocols relating to the prevention and suppression of international terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. It has signed and ratified the UN Convention against Corruption. The UAE ratified the UN Convention against Transnational Organized Crime on May 7, 2007. The UAE supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) in November 2004, and will assume its presidency for 2008.

International Monetary Fund (IMF) conducted an assessment of the UAE financial system in 2007. The report concluded that the government of the UAE is in the midst of implementing an important agenda for further strengthening the country's banking system and its prudential and regulatory oversight. The report contains no information on the UAE compliance with the FATF's 40 recommendations and Nine Special Recommendations.

The Government of the UAE has shown some progress in enhancing its AML/CTF program. Information sharing between the AMLSCU and foreign FIUs has substantially improved. However, several areas requiring further action by the UAEG remain. Law enforcement and customs officials need to proactively recognize money laundering activity and develop cases based on investigations, rather than wait for case referrals from the AMLSCU that are based on SARs. Additionally, law enforcement and customs officials should conduct more thorough inquiries into large and undeclared cash imports into the country, as well as require—and enforce—outbound declarations of cash and gold. All forms of trade-based money laundering must be given greater scrutiny by UAE customs and law enforcement officials, including customs fraud, the trade in gold and precious gems, commodities used as counter-valuation in hawala transactions, and the misuse of trade to launder narcotics proceeds. The UAE should increase the resources it devotes to investigation of AML/CTF both federally at the AMLSCU and at emirate level law enforcement. The Central Bank should move from the initial phase of hawaladar registration to compliance and enforcement coupled with investigations. The cooperation between the Central Bank and the DFSA needs improvement, and lines of authority need to be clarified. Cabinet Resolution No. 28 of 2007 should help in this regard. The UAE should conduct more follow-ups with financial institutions and the MSA regarding the recent tightening of regulations on charities to ensure their registration at the federal level. The UAE should also continue its regional efforts to promote sound charitable oversight, and engage in a public campaign to ensure all local charities are aware of registration requirements. The IMF recently conducted the UAE's mutual evaluation AML/CTF assessment, which is scheduled for discussion at the April 2008 MENAFATF Plenary and the June 2008 FATF Plenary. The UAE should work toward implementing the recommendations of the IMF assessment upon its completion.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although narcotics are still a major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become

increasingly important. The past few years have witnessed the movement of cash placement away from High Street banks and mainstream financial institutions as these entities have tightened their controls and increased their vigilance. The use of bureaux de change, cash smugglers (into and out of the UK), and traditional gatekeepers (including solicitors and accountants) to move and launder criminal proceeds has been increasing since 2002. Also on the rise are credit/debit card fraud and the purchasing of high-value assets to disguise illegally obtained money.

Criminal proceeds are mostly generated in the large metropolitan areas in the UK. Drug traffickers and other criminals are able to launder substantial amounts of money in the UK despite improved anti-money laundering measures introduced under the 2002 Proceeds of Crime Act (POCA). Much of the money made in the UK benefits criminals who operate in the UK. Cities such as London, Liverpool and Birmingham have large drug markets and also serve as supply points for markets in smaller cities and towns, drawing in significant flows of illicit cash.

According to an analysis by the UK's Serious Organized Crime Agency (SOCA), such crimes in the UK generate about £15 billion (approximately U.S. \$29.3 billion) per annum. Businesses that are particularly attractive to criminals are those with high cash turnovers and those involved in overseas trading. Illicit cash is consolidated in the UK, and then moved overseas where it can more readily enter the legitimate financial system, either directly or by means such as purchasing property. Cash can be smuggled in a number of ways: it can be transported by courier, freight or post and moved through the various points of exit from the UK. Cash smuggling techniques are adaptable; smugglers can easily change techniques if they suspect law enforcement is targeting a particular route or method.

Because cash is the mainstay of the drugs trade, traffickers make extensive use of money transmission agents (MTA), cash smuggling, and Informal Value Transfer Systems ("underground banking") to remove cash from the UK. Heroin proceeds from the UK are often laundered through Dubai en route to traffickers in Pakistan and Turkey. Cocaine proceeds are repatriated to South America via Jamaica and Panama.

As money laundering laws become stricter, money laundering becomes more difficult. Because dealers in the UK generally collect sterling, most traffickers are left with excess small currency (usually £10 notes). This has created cash smuggling operations to move large sums of sterling out of the country. The SOCA analysis suggests that more sterling has exited the UK in recent years than entered due to the relative ease of converting sterling in other countries.

The UK has implemented many of the provisions of the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes has been criminalized by subsequent legislation. Banks and nonbank financial institutions in the UK must report suspicious transactions. The UK underwent a FATF mutual evaluation process in 2006, and the report was accepted by that body in June 2007. The mutual evaluation report (MER) cited many improvements to the anti-money laundering and counter-terrorist financing (AML/CTF) regime since the previous on-site assessment, conducted in 1996. On the 49 recommendations, the UK received 24 ratings of "compliant" and 12 ratings of "largely compliant." Of the 5 core FATF recommendations (Recommendations 1, 5, 10, and 13, Special Recommendations II and IV), the UK's AML/CTF regime was deemed at least compliant in all of them.

In 2001, money laundering regulations were extended to money service bureaux (e.g., bureaux de change, money transmission companies), and in September 2006, the Government published a review of the regulation and performance of money service businesses in preventing money laundering and terrorist financing. Since 2004, more business sectors are subject to formal suspicious activity reporting (SAR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods, such as cars and jewelry. Sectors of the betting and gaming industry that

are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

Following an extensive consultation period in late 2006, Her Majesty's Treasury published Money Laundering Regulations in July 2007. The regulations implement the Directive 2005/60/EC (also known as the Third EU Money Laundering Directive), agreed under the UK's EU Presidency in 2005. The provisions include: extended supervision so that all businesses in the regulated sector comply with money laundering requirements; strict tests of money services businesses; extra checks on customers identified by firms as posing a high risk of money laundering; a requirement to establish the source of wealth of customers who are high ranking public officials overseas; and a strengthened and risk-based regime in casinos, in line with international standards. The regulations took effect December 15, 2007. EU Council Regulation No. 1889/2005, known as the "Cash Controls Regulation", also became applicable in the UK on June 15, 2007. This regulation obliges each EU state to maintain a cash declaration system for every person entering or exiting the EU with 10,000 euros cash or its equivalent in other currencies. The UK employs a written declaration system.

The Proceeds of Crime Act 2002 (POCA) created a new criminal offense, applicable to all regulated sectors, of failing to disclose suspicious transactions in respect to all crimes, not just "serious," narcotics- or terrorism-related crimes, as had previously been the rule. The POCA also expanded investigative powers relative to large movements of cash. Sections 327 to 340 of the Act address possession, acquisition, transfer, removal, use, conversion, concealment or disguise of criminal or terrorist property, inclusive of but not limited to money. The POCA also criminalizes tipping off. The "Money Laundering Regulations 2003," along with amending orders for the POCA and the Terrorism Act, impose requirements on various entities, including attorneys, and introduce a client identification requirement, requirements on internal reporting procedures and training. The introduction of the Fraud Act 2006, which took effect on 15 January 2007, saw significant changes to offenses in the fraud and forgery offence group. Changes were also made to the way in which the police record fraud offenses.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through various intermediaries that often advertise on the Internet and also offer various offshore services. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record-keeping requirements. Individuals typically open nonresident accounts for tax advantages or for investment purposes.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction. The FSA also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving banks. The FSA regulates some 29,000 firms, which include European Economic Area (EEA) firms "passporting" into the UK (firms doing business on a cross-border basis), ranging from global investment banks to very small businesses, and around 165,000 individuals. The FSA also regulates mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply. In October 2006, the financial services sector adopted National Occupational Standards of Competence in the fields of compliance and in anti-money laundering. The 2007 FATF mutual evaluation cited a number of concerns including the enforceability of the guidance to some financial institutions regarding customer due diligence, politically exposed persons, and beneficial ownership.

The Serious Organized Crime and Police Act of 2005 (SOCAP) amended the money laundering provisions in the POCA. One of these changes was the creation of the Serious Organized Crime Agency (SOCA), which houses the UK's financial intelligence unit (FIU). In 2006, SOCA assumed all

FIU functions from the National Criminal Intelligence Service (NCIS). SOCA has three functions: the prevention and detection of serious organized crime; the mitigation of the consequences of such crime; and the function of receiving, storing, analyzing and disseminating information, including suspicious activity reports (SARs). Under the law, SOCA's functions are not restricted to serious or organized crime but are applicable to all crimes, and those functions include assistance to other agencies in their enforcement responsibilities. The number of SARs has steadily increased since the establishment of the SOCA even with the slightly relaxed reporting requirements, that allow banks (but no other obliged entities) to proceed with low value transactions not exceeding 250 pounds (approximately \$500) involving suspected criminal property without requiring specific consent to operate the account. However, the reporting of every such transaction is still required. Additionally, under the SOCAP, foreign acts would no longer be considered money laundering and would not be considered as such if they do not violate the law in the foreign jurisdiction.

The Serious Crime Act 2007 merges ARA's operational arm with the Serious Organised Crime Agency (SOCA) and ARA's training function with the National Policing Improvement Authority (NPIA), as well as extending the powers of civil recovery to wider prosecution authorities and the powers of cash seizure to a wider range of law enforcement bodies. The POCA has enhanced the efficiency of the forfeiture process and increased the recovered amount of illegally obtained assets by consolidating existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creating a civil asset forfeiture system for the proceeds of unlawful conduct. The Assets Recovery Agency (ARA), established to enhance financial investigators' power to request client information from any bank, is a product of this legislation. The Act provides for confiscation orders and for restraint orders to prohibit dealing with property. It also allows for asset recovery of property obtained through or used for unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove that the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The POCA also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof. In light of this, Her Majesty's Revenue and Customs (HMRC) has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. The total value of assets recovered by all agencies under the Act (and earlier legislation) in England, Wales, and Northern Ireland approximately U.S. \$250 million in 2006, a fivefold increase in five years.

In one illustrative case, Operation Labici was an investigation into an organized group of money launderers operating in the UK but controlled from Dubai and Pakistan. They used hawala, to eventually move drug money between the UK, Pakistan and Dubai as well as to and from other countries. The UK end of the organization provided laundering services to UK drug dealers. Records seized showed that almost £15 million (U.S. \$30 million) in cash had been passed. In September 2007 the last of eight men was sentenced as a result of Operation Labici. The main defendant received ten years imprisonment; the eight defendants together received 39 years for money laundering.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual to provide financial or related services, directly or indirectly, to or for the benefit of a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a covered entity to fail to disclose to Her Majesty's Treasury a suspicion that a customer or entity is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets. In March 2006, the Terrorism Act received Royal Assent. This Act aims to impede the encouragement of others to commit terrorist acts, and amends existing legislation by introducing warrants enabling police to search any property owned or controlled by a terrorist suspect. The Act also extends terrorism stop and search powers to cover bays and estuaries, with improved search powers at ports; extends police powers to detain suspects

after arrest for 28 days (although intervals exceeding two days must be approved by a judicial authority); and increases the flexibility of the proscription regime, including the power to proscribe groups that glorify terrorism.

As a direct result of the events of September 11, 2001, the FID established a separate National Terrorist Financing Investigative Unit (NTFIU), controlled by the Metropolitan Police Services (MPS), also known as “Scotland Yard,” to maximize the effect of reports from the regulated sector. The NTFIU chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the NTFIU has seen a threefold increase in staffing levels directly due to the increase in the workload. The Metropolitan Police has responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations.

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record-keeping requirements. The Commission has investigative and administrative sanctioning authority, including the authority to remove management, appoint trustees and place organizations into receivership. The Government intends to revise its reporting requirements to develop a risk-based approach to monitoring with a new serious incident reporting function for charities.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. SOCA is a member of the Egmont Group and has information sharing arrangements in place with the FIUs of the United States, Belgium, France, and Australia. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996, and the two countries signed a reciprocal asset sharing agreement in March 2003. The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding in force between the U.S. Immigration and Customs Enforcement and HM Revenue and Customs.

The United Kingdom has a comprehensive AML/CTF regime. However, as discussed in the FATF mutual evaluation, there are areas that should be further addressed by the authorities. The UK should develop legislation and clearly enforceable implementing regulations to ensure that beneficial owners are identified and verified and that customer due diligence is required and ongoing, regardless of an already established relationship with the client. The UK should also develop clear regulations regarding politically exposed persons as well as correspondent banking relationships. Risk-based measures should be codified and taken, not only in the context of customer due diligence, but also with regard to the identification and treatment of wire transfers, the standards and measures set by the designated nonfinancial businesses and professions, and to more effectively target the resources of the supervisory entities. The 2005 Gambling Act should be amended to require the gaming industry to be covered in the same manner as the financial and designated nonfinancial businesses and professions, including giving the Gambling Commission a full range of sanctions. Authorities should track and examine the effects of the SOCAP change regarding acts and assets in or from foreign jurisdictions, and revisit this legislation to determine whether it has been effective, or whether it has enabled exploitation. Authorities should also ensure the FIU’s operational and authoritative independence.

Uruguay

In the past, Uruguay’s strict bank secrecy laws, liberal currency exchange, capital mobility regulations, and overall economic stability made it a regional financial center vulnerable to money laundering, though the extent and the nature of suspicious financial transactions have been unclear. In 2002,

banking scandals and mismanagement, along with massive withdrawals of Argentine deposits, led to a near collapse of the Uruguayan banking system, significantly weakening Uruguay's role as a regional financial center. This crisis has diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term.

Uruguay is a founding member of the Financial Action Task Force for South America (GAFISUD). Since early 2005, the former director of the Government of Uruguay's (GOU) Center for Training on Money Laundering Issues (CECPLA) has served as the GAFISUD Executive Secretary. In 2005, the IMF concluded a thorough examination of Uruguay's money laundering regime, which also served as a GAFISUD mutual evaluation. The examination recognized Uruguay's advances with its new legislation but pointed out that some regulations still needed to be drafted. It also noted the understaffing of Uruguay's financial intelligence unit (FIU). An IMF risk assessment is planned for March 2008.

Money laundering is criminalized under Law 17.343 of 2001 and Law 17.835 of 2004. Under Law 17.343, predicate offenses include narcotics trafficking; corruption; terrorism; smuggling (value over U.S. \$20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues, and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. Money laundering is considered an offense separate from the underlying crimes. The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Law 17.835 significantly strengthens the GOU's anti-money laundering regime by including specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as provisions for undercover operations and controlled deliveries.

The first arrest and prosecution for money laundering under Law 17.835 occurred in October 2005. The case is still underway. A more recent high profile case, involving money laundering tied to the largest cocaine seizure in Uruguay's history is also underway, with 14 people indicted in September 2006 for money laundering. This case has significantly invigorated the GOU's efforts to fight money laundering and to push for increased reporting of suspicious activities. A more recent case (September 2007), also involving a large cocaine seizure and proceeds from trafficking, is in the initial stages of investigation. There have been no prosecutions in 2007.

Uruguay's FIU, the Financial Information and Analysis Unit (UIAF), is a directorate of the Central Bank. Created in 2000 under Central Bank Circular 1722, the UIAF receives, analyzes, and disseminates suspicious activity reports (SARs). Law 17.835 of 2004 expands the realm of entities required to file SARs, makes reporting of such suspicious financial activities a legal obligation, and confers on the UIAF the authority to request additional related information.

Compliance by reporting entities has increased from 94 SARs in all of 2006 to 98 SARs in just the first half of 2007. While the level of staffing at the UIAF is still not adequate, the Central Bank has hired 3 additional staff for a total of 7 full-time personnel and established a timeline of June 2008 to reach full staffing of 19 people. The recent high profile narcotics money laundering cases have provided a boost to the Central Bank's efforts. In addition, the UIAF is updating its hardware and software systems through funding from the Organization of American States.

Under Law 17.835, all obligated entities must implement anti-money laundering policies, such as thoroughly identifying customers, recording transactions over U.S. \$10,000 in internal databases, and reporting suspicious transactions to the UIAF. This obligation extends to all financial intermediaries, including banks, currency exchange houses, stockbrokers, insurance companies, casinos, art dealers, and real estate and fiduciary companies. Implementing regulations have been issued by the Central Bank for all entities it supervises (banks, currency exchange houses, stockbrokers, and insurance companies), and are being issued by the Ministry of Economy and Finance for all other reporting entities. On November 26, 2007, the Central Bank issued Circular 1.978, which requires financial

intermediary institutions, exchange houses, credit administration companies and correspondent financial institutions to implement detailed anti-money laundering and counter-terrorist financing policies, and report wire transfers over U.S. \$1,000. This circular requires these institutions to pay special attention to business with politically exposed persons (PEPs); persons, companies, and financial institutions from countries that are not members of the Financial Action Task Force (FATF) or a FATF-style regional body; and persons, companies, and financial institutions from countries that are subject to FATF special measures for failure to comply with the FATF Recommendations.

Law 17.835 also extends reporting requirements to all persons entering or exiting Uruguay with over U.S. \$10,000 in cash or in monetary instruments. This measure has resulted in the seizure of over U.S. \$720,000 in undeclared cross-border movements since the declaration requirement entered into force in December 2006.

Three government bodies are responsible for coordinating GOU efforts to combat money laundering: the UIAF, the National Drug Council, and the Center for Training on Money Laundering (CECPLA). The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority for anti-money laundering policy. The Director of CECPLA serves as coordinator for all government entities involved and sets general policy guidelines. The Director defines and implements GOU policies, in coordination with the Finance Ministry and the UIAF. The Ministry of Economy and Finance, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The financial private sector, most of which is foreign-owned, has developed self-regulatory measures against money laundering, such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Despite the power of the courts to confiscate property linked to money laundering, real estate ownership is not publicly registered in the name of the titleholder, complicating efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF and other government agencies must obtain a judicial order to have access to the name of titleholders. The GOU is in the process of implementing a national computerized registry that will facilitate the UIAF's access to titleholders' names. Data is being progressively loaded into the system, with a completion target date of December 2008. The UIAF is already using the loaded data for investigation purposes.

Fiduciary companies called "SAFIs" are also thought to be a convenient conduit for illegal money transactions. As of January 1, 2006, all SAFIs are required to provide the names of their directors to the Finance Ministry. In addition, the GOU implemented a comprehensive tax reform law in July 2007, which prohibited the establishment of new SAFIs as of that date. All existing SAFIs are to be eliminated by 2010. The tax reform law also implemented a personal income tax for the first time in Uruguay.

Offshore banks are subject to the same laws and regulations as local banks, with the GOU requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representative offices of foreign banks. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of the Central Bank, and any share transactions must be authorized by the Central Bank. There are eight free trade zones in Uruguay, all but two being little more than warehouses for regional distribution. The other two house software development firms, back-office operations, call centers, and some light manufacturing/assembly. Some of the warehouse-style free trade zones have been used as transit points for containers of counterfeit goods bound for Brazil and Paraguay.

The GOU states that safeguarding the financial sector from money laundering is a priority, and Uruguay remains active in international anti-money laundering efforts. Uruguay is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. In January 2007, the GOU

ratified the UN Convention against Corruption and the OAS Inter-American Convention against Terrorism. The GOU is a member of GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The USG and the GOU are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively.

Uruguay is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Egmont membership would allow its UIAF greater access to financial information that is essential to its efforts to combat money laundering and terrorist financing. The UIAF plans on presenting its candidacy to the Egmont Group in June 2008, with the sponsorship of Spain, Peru, Argentina and Colombia.

The Government of Uruguay has taken significant steps over the past few years to strengthen its anti-money laundering and counter-terrorist financing regime. The passage of legislation criminalizing terrorist financing places Uruguay ahead of many other nations in the region. The UIAF's future membership in the Egmont Group, as well as the GOU's continued implementation and enforcement of its anti-money laundering and counter-terrorist financing programs, should continue to be priorities for the GOU.

Uzbekistan

Uzbekistan is not an important regional financial center and does not have a well-developed financial system. Legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions except when absolutely required, because of the onerous nature of the Government of Uzbekistan's (GOU) financial control system, the fear of GOU seizure of one's assets, and lack of trust in the banking system as a whole. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. They only deposit funds they are required to deposit and often resort to subterfuge to avoid depositing currency. The Central Bank of Uzbekistan (CBU) states that deposits from individuals have been increasing over the past five years.

Narcotics proceeds are controlled by local and regional drug-trafficking organizations and organized crime. Foreign and domestic proceeds from criminal activity in Uzbekistan are held either in cash, high-value transferable assets, such as gold, property, or automobiles, or in foreign bank accounts.

There is a significant black market for smuggled goods in Uzbekistan. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a considerable problem, increased dramatically. Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries and regions, Iran, India, Korea, the Middle East, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded by narcotics proceeds. It is likely, however, that drug dealers use the robust black market to clean their drug-related money.

Reportedly, the unofficial, unmonitored cash-based market creates an opportunity for small-scale terrorist or drug-related laundering activity destined for internal operations. For the most part, the funds generated by smuggling and corruption are not directly laundered through the banking system but through seemingly legitimate businesses such as restaurants and high-end retail stores. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the Central Bank, Ministry of Finance, General Prosecutor's Office (GPO), and state-owned and controlled banks. Although Uzbek financial institutions are not known to engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in Uzbek soum and U.S. dollars. Moreover, drug dealers and

others can transport their criminal proceeds in cash across Uzbekistan's porous borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Money laundering from the proceeds from drug-trafficking and other criminal activities is a criminal offense. Article 41 of the Law on Narcotic Drugs and Psychotropic Substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics trafficking. GOU officials noted that there have been no related cases thus far in Uzbekistan.

Penalties for money laundering are from ten to fifteen years imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer; conversion; exchange; or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity. Although the law has been in effect for more than five years, there is still insufficient information to fully assess the implementation and use of this legislation. Officials from the State Prosecutor's Office reported that Article 243 does not work well because different judges and attorneys can interpret it in different ways.

The CBU, GPO, and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Banks are required to know, record, and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. All transactions involving sums greater than U.S. \$1,000 in salary expenses for legal entities and U.S. \$500 in salaries for individuals must be tracked and reported to the authorities. The CBU unofficially requires commercial banks to report on private transfers to foreign banks exceeding U.S. \$10,000. Depending on the type and amount of the transaction, banks are required to maintain records for time deposits for a minimum of five years, possibly not sufficient time to reconstruct significant transactions. The law protects reporting individuals with respect to their cooperation with law enforcement entities. However, reportedly, the GOU has not adopted "banker negligence" laws that make individual bankers responsible if their institutions launder money.

A new law to combat money laundering and terrorist financing, passed in 2004, took effect in January 2006. However, in April 2007 the main provisions of the law were suspended by a Presidential decree until January 2013. This essentially means there may not be an effective anti-money laundering law in Uzbekistan for the next six years. The provisions of the law required certain entities to report cash transactions above U.S. \$40,000 (approximately), as well as suspicious transactions. GOU officials claimed that the anti-money laundering law burdened banks and investigators with reporting thousands of benign suspicious transactions that wasted resources on investigations. They reported 17,000 suspicious transactions in a six-month period before the law was suspended compared with 400 in the six months following the suspension of the law. In addition, this law also covered some nonbanking financial institutions, such as investment foundations, depositaries and other types of investment institutions; stock exchanges; insurers; organizations which render leasing and other financial services; organizations of postal service; pawnshops; lotteries; and notary offices. It did not include intermediaries such as lawyers, accountants, or broker/dealers. Casinos are illegal in Uzbekistan.

An April 2006 Presidential decree established the Department on Combating Tax, Currency Crimes and Legalizations of Criminal Proceeds under the GPO. The Department, which the Government of Uzbekistan claims is the functional equivalent of a Financial Intelligence Unit (FIU), is charged with monitoring and preventing money laundering and terrorist financing. It analyzes information received from banks and financial institutions, creates and keeps electronic databases of financial crimes, and, when warranted, passes information to the CBU, tax and law enforcement authorities, or other parts of the GPO for investigation and prosecution of criminal activity. However, given the suspension of the

main provisions of the anti-money laundering law in 2007, it is unclear whether there will be any investigations or prosecutions.

The Law on Banks and Bank Activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, private bank information can be disclosed to prosecution and investigation authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently under consideration. Protected banking information also can be disclosed to tax authorities in cases involving the taxation of a bank's client. Additionally, under the 2006 Presidential decree and subsequent Cabinet of Ministers' resolution on the disclosure of information related to money laundering, it is mandatory for organizations involved in transactions with monetary funds and other property to report such transactions to the GPO's FIU. GOU officials noted that the secrecy law does not apply if a group is on a list of designated terrorist organizations.

Existing controls on transportation of currency across borders would, in theory, facilitate detection of the international transportation of illegal source currency. When entering or exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and nonresidents may bring the equivalent of U.S. \$10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Nonresidents may take out as much currency as they brought in. However, residents are limited to the equivalent of U.S. \$2,000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over U.S. \$2,000 must be approved by an authorized commercial bank, and amounts over U.S. \$5,000 must be approved by the CBU. International cash transfers to or from an individual person are limited to U.S. \$5,000 per transaction; there is no monetary limit on international cash transfers made by legal entities, such as a corporation. However, direct wire transfers to or from other Central Asian countries are not permitted; a third country must be used.

International business companies are permitted to have offices in Uzbekistan and are subject to the same regulations as domestic businesses, if not stricter. Offshore banks are not present in Uzbekistan and other forms of exempt or shell companies are not officially present.

The Department of Investigation of Economic Crimes within the Ministry of Internal Affairs (MVD) conducts investigations of all types of economic offenses. A specialized structure within the NSS and the Department on Tax, Currency Crimes and Legalization of Criminal Proceeds is also authorized to conduct investigations of money laundering offenses. Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. Officials from the Office of the State Prosecutor reported that there were 11 money laundering-related cases in 2006 and five in 2007. Of these 16 recent cases, officials stated that three are still pending. The status or disposition of the other cases is unknown. Overall, the GOU appears to lack a sufficient number of experienced and knowledgeable agents to investigate money laundering.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee on the Protection of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism. The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list

and the names of individuals and entities included on the UN 1267 consolidated list. In addition, the GOU has circulated the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to the CBU, which has, in turn, forwarded these lists to banks operating in Uzbekistan. According to the CBU and the Office of the State Prosecutor, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate or deter alternative remittance systems such as hawala, black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems. GOU officials noted that most overseas migrants work in more advanced countries such as Russia or Korea where remittances can be easily tracked through financial institutions. We are not aware of any legislative initiatives under consideration. Although officially there is complete currency convertibility, in reality convertibility requests can be significantly delayed or refused.

The GOU closely monitors the activities of charitable and nonprofit entities, such as NGOs, that can be used for the financing of terrorism. In February 2004, the Cabinet of Ministers issued Decree 56 to allow the government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the degree of supervision of charities and other nonprofits, and the level of threat Uzbekistan perceives from the Islamic Movement of Uzbekistan (IMU) and other extremist organizations, it is extremely unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOs.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Current laws include the ability to seize items used in the commission of crimes such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for “civil” proceedings within the criminal case to decide forfeiture issues. As a practical matter, these proceedings are conducted as part of the criminal case. We are aware of no new legislation or changes in current law under active consideration by the GOU regarding seizure or forfeiture of assets. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan set up a fund to direct confiscated assets to law enforcement activities. In accordance with the regulation, the assets derived from the sale of confiscated proceeds and instruments of drug-related offenses were transferred to this fund to support entities of the NSS, the MVD, the State Customs Committee, and the Border Guard Committee, all of which are directly involved in combating illicit drug trafficking. According to the GOU, a total of 115 million soum (approximately U.S. \$97,000) has been deposited into this fund since its inception. Roughly U.S. \$80,000 has been turned over to Uzbek law enforcement agencies. In 2004, however, the Cabinet of Ministers issued an order to close the Special Fund as of November 1, 2004. Under the new procedure, each agency manages the assets it seizes. There is also a specialized fund within the MVD to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses such as the organization of criminal associations, bribery and racketeering. The GOU enthusiastically enforces existing drug-related asset seizure and forfeiture laws. The GOU has not been forthcoming with information regarding the total dollar value of assets seized from crimes. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

The GOU realizes the importance of international cooperation in the fight against drugs and transnational organized crime and has made efforts to integrate the country in the system of

international cooperation. Uzbekistan has entered into agreements with Uzbek supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Uzbekistan has entered into bilateral agreements for cooperation or exchange of information on drug related issues with the United States, Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the Commonwealth of Independent States (CIS), and all the countries in Central Asia. It has multilateral agreements in the framework of the CIS, under the Shanghai Cooperation Organization, and under memoranda of understanding. An “Agreement on Narcotics Control and Law Enforcement Assistance” was signed with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004.

Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan and the United States have reached informal agreement on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. In the past, Uzbekistan has cooperated with appropriate law enforcement agencies of the USG and other governments investigating financial crimes and several important terrorist-related cases. However, cooperation in these areas has become increasingly problematic in an atmosphere of strained U.S.-Uzbekistan bilateral relations. Uzbekistan joined the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), a FATF-style regional body, at the group’s December 2005 plenary meeting. The EAG will conduct a mutual evaluation of Uzbekistan in 2008, which will include an analysis of Uzbekistan’s decision to suspend the key provisions of the money laundering law.

The GOU is an active party to the relevant agreements concluded under the CIS, the Central Asian Economic Community (CAEC), the Economic Cooperation Organization (ECO), the Shanghai Cooperation Organization, and the “Six Plus Two” Group on Afghanistan. Uzbekistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Uzbekistan has yet to become a party to the UN Convention against Corruption.

A lack of trained personnel, resources, and modern equipment continues to hinder Uzbekistan’s efforts to fight money laundering and terrorist financing. Moreover, the April 2007 decree suspending the main provisions of the money laundering law until 2013 is likely to result in major setbacks. The GOU should rescind this decree, reinstating the provisions of the law, while continuing to refine its pertinent legislation to bring it up to international standards. Additional refinements should expand the cross-border currency reporting rules to cover the transfer of monetary instruments, and precious metals and gems. Access to financial institution records should be given to appropriate regulatory and law enforcement agencies so that they can properly conduct compliance examinations and investigations. While the establishment of an FIU was a positive step in 2006, much will depend, in the future, on the unit’s ability to effectively cooperate with other GOU law enforcement and regulatory agencies in receiving and disseminating information on suspicious transactions. In the short term, FIU operations will depend on whether there is any incoming reporting activity at all, given the suspension of the law.

Vanuatu

Vanuatu’s offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict banking secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation. The GOV passed amendments to four of its main pieces of legislation relative to money laundering and terrorist

financing during its last session of Parliament in November 2005. The four pieces of legislation affected are the Mutual Assistance in Criminal Matters Act No. 31 of 2005, the Financial Transaction Reporting Act No. 28 of 2005, the Counter-Terrorism and Transnational Organized Crime Act No. 29 of 2005, and the Proceeds of Crime Act (Amendment) Act No. 30 of 2005. The International Companies Act was amended in 2006. Taken with Ministerial Order No. 15 (April 2007), this amendment immobilized Bearer Shares and required the identification of Bearer Share custodians.

Vanuatu's financial sector includes five domestic licensed banks (that carry out domestic and offshore business); one credit union; eight international banks; seventy insurance companies (both life and general); and eight foreign exchange instrument dealers, money remittance dealers and bureaux de change, all of which are regulated by the Reserve Bank of Vanuatu. Since the passage of the International Banking Act of 2002, the Reserve Bank of Vanuatu regulates the offshore banking sector that includes the eight international banks and approximately 3,603 international business companies (IBCs), as well as offshore trusts and captive insurance companies. These institutions were once regulated by the Financial Services Commission. IBCs are now registered with the Vanuatu Financial Services Commission (VFSC). This change was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "noncompliant" with many international standards.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act No. 4 of 2002, and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Financial Transaction Reporting Act (FTRA) of 2000 established the Vanuatu Financial Intelligence Unit (VFIU) within the State Law Office. Under the Financial Transactions Reporting (Amendment) Act No. 28 of 2005, the VFIU has a role in ensuring compliance by financial services sector with financial reporting obligations. The VFIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The VFIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations. The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial transaction: the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction.

Although the amendments have been withdrawn from Parliament twice, the FTRA amendments were finally passed in November 2005 and enacted in late February 2006. The amendments include mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. In addition to STR filings, financial institutions will now be required to file currency transaction reports (CTRs) that involve any single transaction in excess of Vanuatu currency Vatu (VT) 1,000,000, or its equivalent in a foreign currency, and wire transfers into and out of Vanuatu in excess of VT 1,000,000 (approximately U.S. \$9,100). The amendments also require financial institutions to maintain internal procedures to implement reporting requirements, appoint compliance officers, establish an audit function to test their anti-money laundering and counter-terrorist financing procedures and systems, as well as provide the VFIU a copy of their internal procedures. Failure to do so will result in a fine or imprisonment for an

individual, or a fine in the case of a corporate entity. The amendments supersede any inconsistent banking or other secrecy provisions and clarify the VFIU's investigative powers.

The amended FTRA defines financial institutions to include casinos licensed under the Casino Control Act No.6 of 1993, lawyers, notaries, accountants and trust and company service providers. The scope of the legislation is so broad that entities such as car dealers and various financial services that currently do not exist in Vanuatu (and are unlikely to in the future) are covered. Applications by foreigners to open casinos are subject to clearance by the Vanuatu Investment Promotion Authority (VIPA) which reviews applications and conducts a form of due diligence on the applicant before issuing a certification to the Department of Customs and Inland Revenue to issue an appropriate license. The Department of Customs and Inland Revenue receives applications from local applicants directly.

The Vanuatu Police Department and the VFIU are the primary agencies responsible for ensuring money laundering and terrorist financing offences are properly investigated in Vanuatu. The Public Prosecutions Office (PPO) is responsible for the prosecution of money laundering and terrorist financing offences. The Vanuatu Police Department has established a Transnational Crime Unit (TCU), and is responsible for investigations involving money laundering and terrorist financing offences, the identification and seizure of criminal proceeds, as well as conducting investigations in cooperation with foreign jurisdictions.

Supervision of the financial services sector is divided between three main agencies: the Reserve Bank of Vanuatu (RBV), the Vanuatu Financial Services Commission (VFSC) and the Customs and Revenue Branch of the Ministry of Finance. The RBV is responsible for supervising and regulating domestic and offshore banks. The VFSC supervises insurance providers, credit unions, charities and trust and company service providers, but is unable to issue comprehensive guidelines or to regulate the financial sectors for which it has responsibility. The Customs and Revenue Branch issues operating licenses.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) retained the criminalization of the laundering of proceeds from all serious crimes, criminalized the financing of terrorism, and included full asset forfeiture, restraining, monitoring, and production powers regarding assets. The Proceeds of Crime Act No. 30 of 2005 through its new Section 74A effective in November 2005, required all incoming and outgoing passengers to and from Vanuatu to declare to the Department of Customs cash exceeding one million VT in possession (approximately U.S. \$9,100).

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence, search and seizure proceedings, forfeiture or confiscation of property, and restraints on dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continued to conduct international banking business after December 31, 2003, in violation of Section 4 of the Act, the licensee is subject to a fine or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international

banking business. Since this time, three international banking businesses have had their licenses revoked.

One of the most significant requirements of the amended legislation is the banning of shell banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. The VFSC has prepared the Trust and Company Services Providers Bill and the GOV will present the bill before Parliament during the first half of 2008. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements, and “fit and proper” requirements. In 2005, Vanuatu enacted Insurance Act No. 54, drafted in compliance with standards set by the International Association of Insurance Supervisors. Insurance Regulation Order No.16 of 2006 was issued on May 2006, and regulates the insurance industry, to include intermediary and agents roles.

International Business Companies (IBC) traditionally could be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protected all information regarding IBCs and provided penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, made IBCs ideal mechanisms for money laundering and other financial crimes. Section 125 of the International Companies Act No. 31 of 1992 (ICA), provided a strict secrecy provision for information disclosure related to shareholders, beneficial ownership, and the management and affairs of IBCs registered in Vanuatu. This provision, in the past, has been used by the industry to decline requests made by the VFIU for information. However, section 17(3) of the new amended FTRA clearly states that the new secrecy-overriding provision in the FTRA overrides section 125 of the ICA. Moreover, the International Companies (Amendment) Act No. 45 of 2006 (ICA) revised the regime governing IBC operations. Ministerial Order No. 15 of 2007 created a Guideline of Custody of Bearer Shares, which immobilized Bearer Shares and requires the identification of Bearer Share custodians.

In November 2005, Vanuatu passed the Counter-Terrorism and Transnational Organized Crime Act (CTTOCA) No. 29 of 2005. The CTTOCA was brought into force on 24 February 2006. The aim of the Act is to implement UN Security Council Resolutions and Conventions dealing with terrorism and transnational organized crime, to prevent terrorists from operating in Vanuatu or receiving assistance through financial resources available to support the activities of terrorist organizations, and to criminalize human trafficking and smuggling. Terrorist financing is criminalized under section 6 of the CTTOCA. Section 7 of the CTTOCA makes it an offence to “directly or indirectly, knowingly make available property or financial or other related services to, or for the benefit of, a terrorist group.” The penalty upon conviction is a term of imprisonment of not more than 25 years or a fine of not more than VT 125 million (U.S. \$1,000,000), or both. Section 8 criminalizes dealing with terrorist property. The penalty upon conviction is a term of imprisonment of not more than 20 years or a fine of not more than VT 100 million (U.S. \$876,500), or both. There were no terrorist financing or terrorism-related prosecutions or investigations in 2006.

In addition to its membership the Asia Pacific Group on Money Laundering, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. The GOV acceded to the UN International Convention for the Suppression of the Financing of Terrorism in October 2005, and acceded to both the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention in January 2006. The GOV has not yet signed the UN Convention against Corruption. The VFIU has a memorandum of understanding with Australia.

In March 2006, the APG conducted a mutual evaluation of Vanuatu, the results of which were reported at the APG plenary meeting in November 2006. The APG evaluation team found that

Vanuatu had improved its anti-money laundering and counter-terrorist financing regime since its first evaluation in 2000 by criminalizing terrorist financing, requiring a wider range of entities to report to the VFIU and enhancing supervisory oversight of obligated entities. However, some deficiencies remain: the GOV has not taken a risk-based approach to combating money laundering and terrorist financing; a person who commits a predicate offense for money laundering cannot also be charged with money laundering; and current law does not require the names and addresses of directors and shareholders to be provided upon registration of an IBC.

The Government of Vanuatu should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards. The GOV should also establish a viable asset forfeiture regime and circulate the updated UNSCR 1267 Sanctions Committee updated list of designated terrorist entities.

Venezuela

Venezuela is one of the principal drug-transit countries in the Western Hemisphere, with an estimated 250 metric tons of cocaine passing through the nation annually. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering regime, refusal to cooperate with the United States on counternarcotics activities, and rampant corruption throughout the law enforcement, judicial, banking, and banking regulatory sectors continue to make Venezuela vulnerable to money laundering. The main sources of money laundering are from proceeds generated by cocaine and heroin trafficking organizations and the embezzlement of dollars from the petroleum industry. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. It is reported that many of these black market traders ship their wares through Venezuela's Margarita Island free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island.

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 49 banks, primarily serves the domestic market. All but one of these banks belong to the Venezuelan Association of Banks. Membership is voluntary and meetings are held monthly.

Money laundering in Venezuela is criminalized under the 2005 Organic Law against Organized Crime. Under the Organic Law against Organized Crime, money laundering is an autonomous offense, punishable by a sentence of eight to twelve years in prison. Those who cannot establish the legitimacy of possessed or transferred funds, or are aware of the illegitimate origins of those funds, can be charged with money laundering, without any connection to drug trafficking. In addition to establishing money laundering as an autonomous predicate offense, the Organic Law against Organized Crime broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques, such as the use of undercover agents. This law, coupled with the Law Against the Trafficking and Consumption of Narcotics and Psychotropic Substances, effectively brings Venezuela's Penal Code in line with the 1988 UN Drug Convention.

In spite of the advances made with the passage of the Organic Law against Organized Crime in 2005, major gaps remain. Two years after promulgation, not a single case has been tried under the new law. Many, if not most, judicial and law enforcement officials remain ignorant of the Law against Organized Crime and its specific provisions, and the financial intelligence unit (FIU) does not have the necessary autonomy to operate effectively. Widespread corruption within the judicial and law enforcement sectors also undermines the effectiveness of the law as a tool to combat the growing

problem of money laundering. Finally, there is little evidence that the Government of Venezuela (GOV) has the will to effectively enforce the legislation it has promulgated.

Under the Organic Law against Organized Crime and Resolution 333-97 of the Superintendent of Banks and Other Financial Institutions (SBIF), anti-money laundering controls have been implemented requiring strict customer identification requirements and the reporting of both currency transactions over a designated threshold and suspicious transactions. These controls apply to all banks (commercial, investment, mortgage, and private), insurance and reinsurance companies, savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, frontier foreign currency dealers, casinos, real estate agents, construction companies, car dealerships, hotels and the tourism industry, travel agents, and dealers in precious metals and stones. These entities are required to file suspicious and cash transaction reports with Venezuela's FIU, the Unidad Nacional de Inteligencia Financiera (UNIF). Financial institutions are required to maintain records for a period of five years.

The UNIF was created under the SBIF in July 1997 and began operating in June 1998. Under the original draft of the Organic Law against Organized Crime, the UNIF would have become an autonomous entity with investigative powers, independent of the SBIF, but the relevant clauses were removed just prior to the law's passage. The UNIF has a staff of approximately 31 and has undergone multiple bureaucratic changes, with five different directors presiding over the UNIF since 2004. The SBIF and the UNIF are viewed dubiously within the financial sector, with credible reports indicating that both are used by the government to investigate political opponents.

The UNIF receives reports on currency transactions (CTRs) exceeding approximately U.S. \$10,000 and suspicious transaction reports (STRs) from institutions regulated by the SBIF: the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, the Bank Deposits and Protection Guarantee Fund, and other nonregulated entities now included under the Organic Law against Organized Crime. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks. Some institutions regulated by the SBIF, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. The SBIF also allows certain customers of financial institutions—those who demonstrate “habitual behavior” in the types and amounts of transactions they conduct—to be excluded from currency transaction reports filed with the UNIF. SBIF Circular 3759 of 2003 requires financial institutions that fall under the supervision of the SBIF to report suspicious activities related to terrorist financing; however, terrorist financing is not a crime in Venezuela.

In addition to STRs and CTRs, the UNIF also receives reports on the domestic transfer of foreign currency exceeding U.S. \$10,000, the sale and purchase of foreign currency exceeding U.S. \$10,000, and summaries of cash transactions that exceed approximately U.S. \$2,100. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. A system has been developed for electronic receipt of CTRs, but STRs must be filed in paper format. Obligated entities are forbidden to reveal reports filed with the UNIF or suspend accounts during an investigation without official approval, and are also subject to sanctions for failure to file reports with the UNIF.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). No statistics are available on the number of STRs or CTRs received in 2007. According to the UNIF, it forwards approximately 30 percent of the STRs it receives to the Attorney General's Office. The Attorney General's office subsequently opens and oversees the criminal investigation. The Venezuelan constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, the SBIF,

or the Attorney General's office, a judge can waive these rights, making Venezuela one of least restrictive countries in Latin America from an investigatorial standpoint.

Prior to the passage of the 2005 Organic Law against Organized Crime, there was no special prosecutorial unit for the prosecution of money laundering cases under the Attorney General's office, which is the only entity legally capable of initiating money laundering investigations. As a result of the limited resources and expertise of the drug prosecutors who previously handled money laundering investigations, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. The Organic Law against Organized Crime calls for a new unit to be established, the General Commission against Organized Crime, with specialized technical expertise in the analysis and investigation of money laundering and other financial crimes. This commission has not been established to date. The Organic Law against Organized Crime also expanded Venezuela's mechanisms for freezing assets tied to illicit activities. A prosecutor may now solicit judicial permission to freeze or block accounts in the investigation of any crime included under the law. However, to date there have been no significant seizures of assets or successful money laundering prosecutions as a result of the law's passage.

The 2005 Organic Law against Organized Crime counts terrorism as a crime against public order and defines some terrorist activities. The law also establishes punishments for terrorism of up to 20 years in prison. However, the Organic Law against Organized Crime does not establish terrorist financing as a separate crime, nor does it provide adequate mechanisms for freezing terrorist assets.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. However, if the GOV does not criminalize the financing of terrorism, the UNIF faces suspension from the Egmont Group in June 2008. Due to the unauthorized disclosure of information provided to the UNIF by the Financial Crimes Enforcement Network (FinCEN), the United States FIU, FinCEN suspended information exchange with the UNIF in January 2007. FinCEN and the UNIF are currently negotiating a Memorandum of Understanding (MOU) that outlines the parameters for future information exchange between the two FIUs. Once signed, FinCEN will begin sharing financial intelligence with the UNIF again.

Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Money Laundering Experts Working Group and is a member of the Caribbean Financial Action Task Force (CFATF). The GOV is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the OAS Inter-American Convention against Terrorism. The GOV has signed, but not yet ratified, the UN Convention against Corruption. The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991. Venezuela and the United States signed a Mutual Legal Assistance Treaty (MLAT) in 1997, but it has not entered into force.

The Government of Venezuela took no significant steps to expand its anti-money laundering regime in 2007. There were no prosecutions or convictions for money laundering in 2007, and this is unlikely to change in 2008. The 2005 passage of the Organic Law against Organized Crime was a step towards strengthening the GOV's abilities to fight money laundering. However, Venezuela needs to enforce the law by creating procedures to expedite asset freezing, establishing an autonomous financial investigative unit, and ensuring that law enforcement and prosecutors have the necessary expertise and resources to successfully investigate and prosecute money laundering cases. The GOV should also criminalize the financing of terrorism and establish procedures for freezing terrorist assets. The UNIF should sign the MOU with FinCEN that will allow it to resume sharing financial intelligence with the

United States, and take the necessary steps to ensure that information exchanged with other financial intelligence units is subject to the appropriate safeguards mandated by the Egmont Group.

Vietnam

Vietnam is not an important regional financial center, but is the site of significant money laundering activities. Vietnam remains a largely cash-based economy and both U.S. dollars and gold are widely used as a store of value and means of exchange. Remittances are a large source of foreign exchange, exceeding annual disbursements of development assistance and rivaling foreign direct investment in size. Remittances from the proceeds of narcotics in Canada and the United States are also a source of money laundering as are proceeds attributed to Vietnam's role as a transit country for narcotics.

The Vietnamese banking sector is in transition from a state-owned to a partially privatized industry. At present, approximately 80 percent of the assets of the banking system are held by state-owned commercial banks that allocate much of the available credit to state-owned enterprises. Almost all trade and investment receipts and expenditures are processed by the banking system, but neither trade nor investment transactions are monitored effectively. As a result, the banking system could be used for money laundering either through over or under invoicing exports or imports or through phony investment transactions. Official inward remittances in the first six months of 2007 were estimated to be approximately \$2.8 billion. These amounts are generally transmitted by wire services and while officially recorded, there is no reliable information on either the source or the recipients of these funds. Financial industry experts believe that actual remittances may be double the official figures. There is evidence that large amounts of cash are hand carried into Vietnam, which is legal as long as the funds are declared. The Government of Vietnam (GOV) does not require any explanation of the source or intended use of funds brought into the country in this way. In 2006, Vietnam Airlines was implicated in a U.S. \$93 million money laundering scheme uncovered by the Australian Crime Commission. Vietnamese organized crime syndicates operating in Australia and involved in money transfer businesses used the airline to help smuggle money to Vietnam.

A form of informal value transfer service, which often operates through the use of domestic jewelry and gold shops, is widely used to transfer funds within Vietnam. Money or value transmitters are defined as financial institutions by Decree No. 74 and are therefore subject to its AML-related provisions; however, the informal transmitters have not been brought under regulation or supervision.

The U.S. Drug Enforcement Agency (DEA) is engaged in a number of investigations targeting significant ecstasy and marijuana trafficking organizations, composed primarily of Vietnamese legal permanent residents in the United States and Vietnamese landed immigrants in Canada as well as naturalized U.S. and Canadian citizens. These drug trafficking networks are capable of laundering tens of millions of dollars per month back to Vietnam, exploiting U.S. financial institutions to wire or transfer money to Vietnamese bank and remittance accounts, as well as engaging in the smuggling of bulk amounts of U.S. currency and gold into Vietnam. The drug investigations have also identified multiple United States-based money remittances businesses that have remitted over \$100 million annually to Vietnam. It is suspected that the vast amount of that money is derived from criminal activity. Law enforcement agencies in Australia and the United Kingdom have also tracked large transfers of drug profits back to Vietnam.

Article 251 of the Amended Penal Code criminalizes money laundering. The Counter-Narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the "legalizing" (i.e., laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and, it gives the Ministry of Public Security's specialized counter narcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The Penal Code governs money laundering related offenses and no money laundering cases have yet been prosecuted. Article 251 does not meet current

international standards and amongst other weaknesses, the law requires a very high burden of proof (essentially, a confession) to pursue AML allegations, so prosecutions are nonexistent and international cooperation is extremely difficult. The GOV has plans to revise Article 251 and present the draft to Parliament in 2008.

In June 2005, GOV issued Decree 74/2005/ND-CP on Prevention and Combating of Money Laundering. The Decree covers acts committed by individuals or organizations to legitimize money or property acquired from criminal activities. The Decree applies to banks and nonbank financial institutions. The State Bank of Vietnam (SBV) and the Ministry of Public Security (MPS) take primary responsibility for preventing and combating money laundering. Neither the Penal Code, nor the decree covers counterterrorist finance. Reportedly, the Prime Minister has discussed the possibility of dealing with terrorist financing through issuance of a government directive. However, such a directive would have no penal force.

The SBV supervises and examines financial institutions for compliance with anti-money laundering/counter terrorist financing regulations. Financial institutions are responsible for knowing and recording the identity of their customers. They are required to report cash transactions conducted in one day with aggregate value of Vietnam Dong (VND) 200 million (approximately U.S. \$13,000) or more, or equivalent amount in foreign currency or gold. The threshold for savings transactions is VND 500 million (approximately U.S. \$31,000). Furthermore, financial institutions are required to report all suspicious transactions. Banks are also required to maintain records for seven years or more. Banks are responsible for keeping information on their customers secret, but they are required to provide necessary information to law enforcement agencies for investigation purposes.

Foreign currency (including notes, coins and traveler's checks) in excess of U.S. \$7,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of U.S. \$7,000 (or its equivalent in other foreign currencies) is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The 2005 Decree on Prevention and Combating of Money Laundering provides for provisional measures to be applied to prevent and combat money laundering. Those measures include 1) suspending transactions; 2) blocking accounts; 3) sealing or seizing property; 4) seizing violators of the law; and, 5) taking other preventive measures allowed under the law.

The 2005 Decree also provides for the establishment of an Anti-Money Laundering Information Center (AMLIC) under the State Bank of Vietnam (SBV). Similar to a Financial Intelligence Unit (FIU), the AMLIC will function as the sole body to receive and process financial information. It will have the right to request concerned agencies to provide information and records for suspected transactions. The AMLIC was formally established and began operations since February 2006. The Director of the center is appointed by the Governor of the SBV and reports directly to the Governor on anti-money laundering issues. SBV acts as the sole agency responsible for negotiating, concluding and implementing international treaties and agreements on exchange of information on transactions related to money laundering.

The AMLIC staff is currently split between two office locations with only two computers for its staff members. The Center has 13 full time staff members, and is working to hire more. The AMLIC has established liaison with ministries and agencies such as Ministries of Justice, Public Security, Finance, Foreign Affairs, the Supreme People's Procuracy, the Supreme People's Court, and the Banking Association. Since the Center became operational, it has received 20 suspicious transaction reports and has referred six cases to MPS for investigation. The AMLIC has virtually no IT capacity and a very low level of analytical ability.

The MPS is responsible for investigating money laundering related offences. There is no information from MPS on investigations, arrests, and prosecutions for money laundering or terrorist financing, but the SBV reports that there have been no arrests or prosecutions for money laundering since January 1, 2007. MPS is responsible for negotiating and concluding international treaties on judicial assistance, cooperation and extradition in the prevention and combat of money laundering related offenses. MPS signed a nonbinding Memorandum of Understanding with DEA in 2006 to strengthen law enforcement cooperation in combating transnational drug-related crimes, including money laundering, but claims it is unable to provide such information due to constraints within the Vietnamese legal system. In May 2007, Vietnam became a member of the Asia/Pacific Group on Money Laundering (APG). As a member of APG, Vietnam has committed to a comprehensive review of its AML/CTF regime in 2008.

Vietnam is a party to the 1999 UN International Convention for the Suppression of the Financing of Terrorism. Reportedly, Vietnam plans to draft separate legislation governing counter-terrorist financing, though it will not set a specific time frame for this drafting. Currently SBV circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. No related assets have been identified.

Vietnam is a party to the 1988 UN Drug Convention. Under existing Vietnamese legislation, there are provisions for seizing assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash, though the seizures are usually directly linked to drug crimes. Final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

Vietnam has signed but not ratified either the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. Vietnam is ranked 123 out of 179 countries in Transparency International's 2007 Corruption Perception Index.

The Government of Vietnam should promulgate all necessary regulations to implement fully the 2005 decree on the Prevention and Combating of Money Laundering. Vietnam should also pass legislation to make terrorist financing a criminal offense as well as including provisions governing the prevention and suppression of terrorist financing. Vietnam should ratify the UN Conventions against Transnational Organized Crime and Corruption. Vietnamese law enforcement authorities should investigate money laundering, trade fraud, alternative remittance systems, and other financial crimes in Vietnam's shadow economy. The AMLIC needs to be equipped with an electronic information reporting system. Vietnam should take additional steps to establish an anti-money laundering/counter-terrorist financing regime that comports with international standards.

Yemen

The Yemeni financial system is not well developed and the extent of money laundering is not known. Yemen is not considered an important regional financial center; nor is it considered an offshore financial center. Although financial institutions are technically subject to limited monitoring by the Central Bank of Yemen, in practice, alternative remittance systems, such as hawala, are not subject to scrutiny and are vulnerable to money laundering and other financial abuses. The banking sector is relatively small with 17 commercial banks, including four Islamic banks. All banks are under Central Bank supervision. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen has a large underground economy. The smuggling of trade goods and contraband is profitable. The use of khat is common in Yemen and there have been a number of investigations over the years of khat being smuggled from Yemen and East Africa into the United States with profits laundered and

repatriated via hawala networks. Smuggling and piracy are rampant along Yemen's sea border with Oman, across the Red Sea from the Horn of Africa, and along the land border with Saudi Arabia.

In April 2003 Yemen's Parliament passed anti-money laundering (AML) legislation (Law 35). The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation relating to terrorist financing, although terrorism is covered in various pieces of legislation that treat terrorism and terrorist financing as serious crimes. In November 2007 the Cabinet sent a draft counter-terrorist financing law to Parliament.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of individuals and entities that open accounts (or in the case of the dealers for those who execute a commercial transaction), to keep records of transactions for up to ten years, and to report suspicious transactions (STRs). In addition, the law requires that reports be submitted to the Anti-Money Laundering Information Unit (AMLIU), an information-gathering unit within the Central Bank. This unit acts as the financial intelligence unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC), within the Central Bank.

The AMLC is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, and Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the Central Bank of Yemen, and the Association of Banks. The AMLC is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

There are approximately 448 registered money exchange businesses in Yemen, which serve primarily as currency exchangers in addition to performing funds transfer services. Money transfer businesses are required to register with Central Bank for one permit, but can open offices at multiple locations. Fund transfers that exceed the equivalent of \$10,000 require permission from the Central Bank. The Central Bank has not begun to examine the money exchange business for AML compliance.

The AMLIU is understaffed with only a few employees, although it also uses the services of field inspectors from the Central Bank's Banking Supervision Department. The AMLIU has no database and is not networked internally or to the rest of the Central Bank. The Central Bank provides training to other members of the government to assist in elements of anti-money laundering enforcement, but the lack of capacity hampers any attempts by the AMLIU to control illicit activity in the formal financial sector.

Law 35 also grants the AMLC the ability to exchange information with foreign entities that have signed a letter of understanding with Yemen. The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity.

Prior to passage of the AML law, the Central Bank issued Circular 22008 in April 2002, instructing financial institutions to positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than \$10,000, when they have no accounts at the banks in question. The same provision applies to beneficiaries of such transfers. The circular also prohibits inbound and out-bound money transfer of more than \$10,000 cash without prior permission from the Central Bank, although this requirement is not strictly enforced. Banks must also report suspicious transactions to the AMLIU. The circular is distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "know your customer" procedures and "Core Principles for Effective Banking Supervision". In 2005, two STRs were filed with the AMLIU and in 2006, three STRs were filed. The number of STRs filed in 2007 with the AMLIU is not available. However, in 2007 the AMLIU forwarded one suspicious case to the Office of the Public Prosecutor

for suspected money laundering. There have not been any money laundering prosecutions or convictions in Yemen.

At present, Yemen has no cross-border cash declarations or disclosure requirements. However, according to the Customs Authority, inspectors will fill out a declaration form after money has been discovered leaving or entering the country at the border.

Yemen has one free trade zone (FTZ) in Aden. Identification requirements are enforced. For example, truckers must file the necessary paperwork in relevant trucking company offices and must wear ID badges. FTZ employees must undergo background checks by police, the Customs Authority and employers. There is no evidence that the FTZ is being used for trade-based money laundering or terrorist financing schemes.

In September 2003, the Central Bank responded to the UNSCR 1267 Sanctions Committee's consolidated list, the Specially Designated Global Terrorists by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, by issuing circulars 75304 and 75305 to all banks operating in Yemen. Circulars 75304 and 75305 directed banks to freeze the accounts of 144 persons, companies, and organizations, and to report any findings to the Central Bank. As a result, one account was immediately frozen. In 2006, the CBY began issuing a circular every three months containing an updated list of persons and entities belonging to Al-Qaida and the Taliban. However, since the February 2004 addition of Yemeni Sheikh Abdul Majid Zindani to the UNSCR 1267 Sanctions Committee's consolidated list, the Yemeni government has made no known attempt to enforce the sanctions and freeze his assets. There is no information on whether Yemeni authorities have identified, frozen, seized, or forfeited other assets related to terrorist financing.

The Government of Yemen (GOY) has a forfeiture system in place. A judge must order the forfeiture for the items involved in or proceeds from the crime for which the defendant was convicted. Forfeiture is available for all crimes and extends to funds and property. Authorities deposit forfeited funds into the general treasury unless the funds are the proceeds from a drug offense, in which case the proceeds go to law enforcement authorities, who can use the proceeds to buy vehicles or other equipment. If the court orders a defendant to forfeit property, the judge issues an order to auction off the property to the public, with the funds from the auction going into the general treasury. In some instances, the courts can order real property, such as a dwelling, to be closed for one year before the owner may use it again. Yemen has not yet forfeited any real property.

In 2001 the government enacted a law governing charitable organizations. This law entrusts the Ministry of Social Affairs and Labor (MOSAL) with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established. Central Bank Circular No. 33989 of June 2002 and Circular No. 91737 of November 2004, ordered banks to enhance controls regulating opening and managing charities' accounts. This was in addition to keeping these accounts under continuous supervision in coordination with the MOSAL.

The Central Bank is active in educating the public and the financial sector, including money services businesses and money laundering reporting officers, about the proper ways and means of detecting and reporting suspicious financial transactions.

Yemen is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). There is no information available on Yemen's mutual evaluation by MENAFATF. Yemen is a party to the 1988 UN Drug Convention; it has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. The GOY is a party to the UN Convention against Corruption. Yemen is listed 131 out of 179 countries in Transparency International's 2007 Corruption Perception Index.

The Government of Yemen should continue to develop an anti-money laundering regime that adheres to international standards, including the FATF 40 Recommendations and Nine Special Recommendations on terrorist financing. Banks and nonbank financial institutions should enhance their capacity to detect and report suspicious financial transactions to the FIU. The AMLIU needs substantial improvement of its analytical capabilities. Yemen must investigate the abuse of alternative remittance systems such as hawala networks with regard to money laundering and terrorist financing. Law enforcement and customs authorities should also examine trade-based money laundering and customs fraud. Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. Yemen should enforce sanctions and freeze the assets of Sheikh Abdul Majid Zindani, who was added to the UN 1267 Sanctions Committee's consolidated list in February 2004. Yemen should ratify the UN Convention against Transnational Organized Crime and should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Zimbabwe

Zimbabwe is not a regional financial center, but as economic conditions continue to deteriorate for the eighth straight year, money laundering has become a growing problem. This is a result of official corruption and impunity; a flourishing parallel exchange market; rampant smuggling of precious minerals; widespread evasion of exchange controls by legitimate businesses; and company ownership through nominees. Deficiencies in the Government of Zimbabwe's (GOZ) regulatory and enforcement framework contribute to Zimbabwe's potential as a money laundering destination. These deficiencies include: an understaffed bank supervisory authority; a lack of trained regulators and lack of investigators to investigate and enforce violations and financial crime; financial institutions determined to bypass the regulatory framework; limited asset seizure authority; a laissez-faire attitude toward compliance with the law on the part of elements of the business community; ready acceptance of the U.S. dollar in transactions; and significant gold and diamond exports and illegal gold and diamond trading.

During 2007, the government took some steps to prevent money laundering and illegal smuggling activities, including the installation of a new electronic surveillance system to monitor all transactions in the banking system and launch of an operation targeted at illegal precious minerals mining and trading.

In December 2003, the GOZ submitted the Anti-Money Laundering and Proceeds of Crime Act to Parliament, which enacted the legislation. This bill criminalizes money laundering and implements a six-year record keeping requirement. In 2004, the GOZ adopted more expansive legislation in the Bank Use Promotion and Suppression of Money Laundering Act (the Act) that extends the anti-money laundering law to all serious offenses. The Act mandates a prison sentence of up to fifteen years for a conviction. It also criminalizes terrorist financing and authorizes the tracking and seizure of assets. The Act has reportedly raised human rights concerns due to the GOZ's history of selective use of the legal system against its opponents, but its use to date has not been associated with any reported due process abuses or provoked any serious public opposition. The Exchange Control Order, enacted in 1996, obligates banks to require individuals who deposit foreign currency into a foreign currency account to submit a written disclosure of sources of the funds.

The Reserve Bank of Zimbabwe (RBZ) is the lead agency for prosecuting money laundering offenses. In May 2006, the RBZ issued new Anti-Money Laundering Guidelines that outline and reinforce requirements established in the Act for financial institutions and designated nonfinancial businesses and professions. These binding requirements make provisions regarding politically exposed persons and include the obligation to gather and make available to regulators more personal data on these high-profile clients. Financial institutions must now keep records of accounts and transactions for at least

ten years, and report any suspicious transactions to the financial intelligence unit (FIU). The Act also criminalizes tipping off. Failure to report suspected money laundering activities or violating rules on properly maintaining customer data carries a possible fine of Zimbabwe \$3 million (approximately U.S. \$100 at the official exchange rate or less than U.S. \$2 at the parallel market rate) for each day during which a financial institution is in default of compliance. During the year, the RBZ, in cooperation with police, launched Operation Chikorokoza Chapera (“No Illegal Panning”) to crack down on rampant illegal gold mining and smuggling. The RBZ reported that it had secured nearly 100 convictions from 221 investigations to date. In November, the government also enacted stiffer penalties for dealing in illegal minerals under the Precious Stones Trade Amendment Bill. Those convicted of illegally possessing or trading in precious minerals now face a penalty of a minimum of five years imprisonment and a fine of up to Zimbabwe \$50 million (approximately U.S. \$1,666 at the official exchange rate or less than \$33 at the parallel market rate).

The 2004 Act provides for the establishment of The Financial Intelligence Inspectorate and Evaluation Unit (FIIE), Zimbabwe’s financial intelligence unit (FIU). The FIIE is housed within the RBZ. The FIIE receives suspicious transaction reports (STRs), issues guidelines, such as the Anti-Money Laundering Guidelines issued in May 2006, and enforces compliance with procedures and reporting standards for obligated entities.

In June 2007, the RBZ installed an electronic surveillance system to track all financial transactions in the banking system. The FIIE reported that after the launch of the new system, there was a noticeable improvement in self-regulation at banks as demonstrated by an increase in the number of STRs received. During the year, the RBZ continued to tightly control limits on daily cash withdrawals for individuals and companies, ostensibly in an effort to curtail money laundering but more likely to inhibit private sector parallel foreign exchange activities. In November 2007, after a sharp devaluation, the Zimbabwe dollar was still trading on the parallel market at a premium of approximately 4,900 percent above the official exchange rate. When requested, the local banking community has cooperated with the GOZ in the enforcement of asset tracking laws. However, increasingly burdensome GOZ regulations and the resulting hostile business climate have led to growing circumvention of the law by otherwise legitimate businesses. In May, the RBZ cancelled the foreign currency exchange license of NMB Bank, the first indigenous bank in Zimbabwe, after a senior NMB official allegedly externalized more than U.S. \$4.5 million in embezzled funds and fled the country. RBZ cited a breach of Exchange Control Regulations and a failure to report suspicious transactions as required under the Act.

The GOZ continued to arrest prominent Zimbabweans for activities that it calls “financial crimes.” Prosecutions for such crimes, however, have reportedly been selective and politically motivated. The government often targets persons who have either fallen out of favor with the ruling party, or individuals without high-level political backing. Most financial crimes involved violations of currency restrictions that criminalize the externalization of foreign exchange. In light of the inability of the vast majority of businesses to access foreign exchange from the RBZ, most companies privately admit to externalizing their foreign exchange earnings or to accessing foreign currency on the parallel market. Moreover, the GOZ itself, through the RBZ, has been a major purchaser of foreign currency on the parallel market.

In August 2006, the GOZ implemented a currency re-denomination program that slashed three zeros from Zimbabwe’s currency (so that Z\$100,000 became Z\$100). The purpose of the campaign was to ease bookkeeping and the handling of cash transactions under runaway inflation and at the same time assert greater GOZ control over the financial sector. Although the campaign had nothing to do with cracking down on money laundering, when the holder of cash could not prove a legitimate source of funds, the cash was deposited into zero-interest “anti-money laundering coupons,” and the case was referred to the RBZ’s Suppression of Money Laundering Unit for further investigation. The government claimed that more than 2,000 persons were arrested for “money laundering” in this period

and charged under the Exchange Control Act. The government has not provided any additional information about the status or resolution of any of these cases.

The 2001 Serious Offenses (Confiscation of Profits) Act establishes a protocol for asset forfeiture. The Attorney General may request confiscation of illicit assets. The Attorney General must apply to the court that has rendered the conviction within six months of the conviction date. The court can then issue a forfeiture order against any property. Despite the early date of this law compared to the money laundering legislation that followed, this law does define and incorporate money laundering among the bases for the GOZ to confiscate assets.

With the country in steep economic decline and increasingly isolated, Zimbabwe's laws and regulations remained ineffective in combating money laundering. The government's anti-money laundering efforts throughout the year appeared to be directed more at securing the government's own access to foreign currency, targeting opponents, and tightening control over precious minerals than to ensuring compliance. Despite having the legal framework in place to combat money laundering, the sharp contraction of the economy, growing vulnerability of the population, and decline of judicial independence raise concerns about the capacity and integrity of Zimbabwean law enforcement. Transparency International ranks the Government of Zimbabwe at 150 of 179 countries on its 2007 Corruption Perceptions Index. The banking community and the RBZ have cooperated with the United States in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention. In March 2007, the Zimbabwe Parliament ratified the UN Convention against Corruption. However, Zimbabwe has yet to ratify the UN Convention against Transnational Organized Crime and the African Union Convention against Corruption, and has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in 2003 and assumed the Presidency for ESAAMLG for the 2006/2007 administrative year. Zimbabwe experienced the first completed mutual evaluation undertaken by ESAAMLG. The report was accepted at the plenary and Council of Ministers meeting in August 2007.

The GOZ leadership should work to develop and maintain transparency, prevent corruption, and to subscribe to practices ensuring the rule of law. The GOZ must also work toward reducing the rate of inflation, halting the economic collapse, and rebuilding the economy to restore confidence in the currency. The GOZ can illustrate its commitment to combating money laundering and terrorist financing by using its legislation for the purposes for which it was designed, instead of using it to persecute opponents of the regime and nongovernmental organizations with which it opposes. Once these basic prerequisites are met, the GOZ should endeavor to develop and implement an anti-money laundering/counter-terrorist financing regime that comports with international standards. The GOZ should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism, and should ratify the African Union Convention against Corruption and the UN Convention against Transnational Organized Crime.